ANALISI DINAMICA MARKE

Kamenica Kristiano

Per migliorare l'analisi dinamica di questo malware, abbiamo integrato l'uso di Process Monitor. Questo strumento ci permette di acquisire una visione dettagliata dei processi in esecuzione durante l'attività del malware.

Con questa aggiunta, saremo in grado di individuare comportamenti sospetti o anomalie nel contesto dell'esecuzione del codice dannoso, fornendoci una comprensione più approfondita delle sue azioni e potenziali rischi per il sistema.

Process Name	PID	Operation	Path	Result	Detail
Malware U3 W2 L2.exe	3372 A	Process Start		SUCCESS	Parent PID: 1608, Command line: "C:\Documents and Settings\Administrator\Desktop\Eserci
Malware_U3_W2_L2.exe	3372	Thread Create		SUCCESS	Thread ID: 3376
Malware_U3_W2_L2.exe	3372	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio Pratico U3 W2 L2\Malware U3 W2 L2 exe	SUCCESS	Name: \Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malw
Mahuare 113 W2 12 eve	3372	Load Image	C:\Documents and Settings:\Administrator\Desktoo\Esercizio Pratico U3 W2 L2\Malware U3 W2 L2 eve	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
Mahuara 113 1s/2 1 2 aug	3372	Load Image	C:\WINDOWS\swstem32\ntdl.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xaf000
Malware_U3_W2_L2.exe Malware_U3_W2_L2.exe	3372	QuenNameInformationFile	C:\Documents and Settings\Administrato\Desktop\Esercizio Pratico U3 W2 L2\Malware U3 W2 L2 exe	SUCCESS	Name: \Documents and Settings\Administrator\Desktop\Esercizio Pratico U3 W2 L2\Malk
Malware U3 W2 L2.exe	3372	CreateFile	C:\WINDOWS\Prefetch\MALWARE U3 W2 L2.EXE-1535026A.pd	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attribu
Mahuara 112 3/2 1 2 aug	3372	QueryStandard nformationFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2_E\E-1535026A.pr	SUCCESS	AllocationSize: 8,192, EndOfFile: 6,536, NumberOfLinks: 1, DeletePending: False, Directory: F
Malware 113 W/2 1.2 eve		ReadFile	C:\WINDOWS\Prefetch\MALWARIE_U3_W2_L2_EXE-1535026A.pd	SUCCESS	Offset 0. Length: 6.536
Mahuare 113 W2 12 eve	3372	ReadFile	C:\WINDOWS\Pheletch\MALWARIE_U3_W2_L2_EXE-1535026A.pl	SUCCESS	Offset: 0, Length: 6,536, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
Malware 113 3/2 1 2 ave		CloseFile	C:\WINDOWS\Pheletch\MALWARE_U3_W2_L2_EXE-1535026A.pf	SUCCESS	
Mahuare 113 1u/2 1 2 eve	3372	CreateFile	C	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize, Disposition: Open, Options: Sy
Malware U3 W2 L2 exe		QuenInformationVolume	C:	SUCCESS	VolumeCreationTime: 3/20/2017 9:34:16 PM, VolumeSerialNumber: D88A-8021, SupportsOb
Malware_U3_W2_L2.exe Malware_U3_W2_L2.exe		FileSystemControl	S	SUCCESS	Control: FSCTL_FILE_PREFETCH
		CreateFile	C/	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory
		QuenDirectory	C/	SUCCESS	0: 65e5bdf5ca391440390554e9ae7b, 1: AUTOEXEC BAT, FileInformationClass: FileNamesIn
Mahoure 113 W2 12 eve		QuenDirectory	C/	NO MORE FILES	3. 44444 A. 4444 A. 444
Mahware 113 W2 12 eve		CloseFile	C/	SUCCESS	
		CreateFile	C-/DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory
Makuare 113 1µ/2 1.2 eve		QueryDirectory	C.VDocuments and Settings	SUCCESS	D 1: FileInformationClass: FileNamesInformation, 3 All Users, 4: Default User, 5: LocalSer
Malware_U3_W2_L2.exe		QueryOrectory	C\Documents and Settings	NO MORE FILES	U. + 1 Patricullidade Catal. Factoristic mountains C.S. All Crists, N. Delouis Crist, S. Cocasca
Malware_U3_W2_L2.exe		CloseFile	C:\Documents and Settings	SUCCESS	
Mahusen 112 14/2 1 2 aug		CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory
Malware_U3_W2_L2.exe		QuenOirectory	C:\Documents and Settings\Administrator	SUCCESS	0:1:, FileInformationClass: FileNamesInformation. 3: Cookies, 4: Desktop, 5: Favorites, 6: I
		QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES	C, I,, Pachsonianoricass. Pachanicsinaumaner, S. Counce, 4. Desixop, S. Pavanes, C. L
Malware_U3_W2_L2.exe Malware_U3_W2_L2.exe		CloseFile	C:\Documents and Settings\Administrator	SUCCESS	
Malware_U3_W2_L2.exe		CreateFile	C. VDocuments and Settings Administrator Desktop	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory
Malware_U3_W2_L2.exe		QuenOirectory	C:\Documents and Settings\Administrator\Desktop	SUCCESS	Time FileInformationClass: FileNamesInformation, 3 CFF Explorer Ink, 4 Command Promote
Malware_U3_W2_L2 exe		QueryOrectory	C. Vocuments and Settings Administrator Desktop C. Vocuments and Settings Administrator Desktop	NO MORE FILES	C., F., Friedrichmanon-Lass: Friedramestinformation, 3: CFF Explorer.nk, 4: Command Prompt
Malware U3 W2 L2 exe		CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	
Malware_U3_W2_L2.exe				SUCCESS	Desired Assess Based Date 8 int Directors Construction Direction Comp. Online. Director
		CreateFile	C:\Documents and Settings\Administrator\Desktop\ESERCIZID_PRATICD_U3_W2_L2		Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory
maiware_U3_W2_L2.exe		QueryDirectory QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	0: ., 1:, FileInformationClass: FileNamesInformation
Malware_U3_W2_L2.exe Malware_U3_W2_L2.exe Malware_U3_W2_L2.exe			C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES	
		CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	
Malware_U3_W/2_L2.exe		CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory
Malware_U3_W2_L2.exe		QueryDirectory	C:\WINDOWS	SUCCESS	0: ., 1:, FileInformationClass: FileNamesInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: asse
Malware_U3_W2_L2.exe		QueryDirectory	C:\WINDOWS	NO MORE FILES	
Malware_U3_W2_L2.exe		CloseFile	C:\WINDOWS	SUCCESS	
Malware U3 W2 L2 eve		CreateFile	C:\WINDOWS\AppPatch	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory
Malware_U3_W2_L2.exe		QueryDirectory	C:\WINDUW5\AppPatch	SUCCESS	0:, 1:, FileInformationClass: FileNamesInformation, 3: AcGenral dll, 4: AcLayers.dll, 5: AcLux
Malware_U3_W2_L2.exe		QuetyDirectory	C:\WINDOW5\AppPatch	NO MORE FILES	
Malware_U3_W2_L2.exe		CloseFile	C:\WINDOW5\AppPaich	SUCCESS	
Malware_U3_W2_L2.exe		CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory
Malware_U3_W2_L2.exe		QueryDirectory	C:\WIND0W5\system32	SUCCESS	 ., 1:, FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1028, 6: 1031, 7: 1033
Malware_U3_W2_L2.exe		QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: eapsvc.dl, 1: edit.com, FileInformationClass: FileNamesInformation, 3: edlin.exe, 4: efsadu.c
		QueryDirectory	C:\WINDOWS\system32	SUCCESS	0; more.com, 1; moricons.dll, FileInformationClass: FileNamesInformation, 3; mouse.div, 4; mp4
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: progman.exe, 1: PRONtObj.dl, FileInformationClass: FileNamesInformation, 3: PROUnstLexi
Malware U3 W2 L2 exe	3372	QueniDirectory	C:\WINDOWS\sestem32	SUCCESS	0: viov.dl. 1; vmGuest_b.dl. FielnformationClass: FileNamesInformation, 3; vmhofs.dl. 4; VML

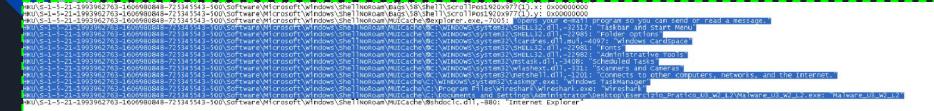
Per arricchire l'analisi delle azioni intraprese dal malware, è interessante notare che, tra le sue attività, si osserva la creazione di file, soprattutto all'interno della directory di sistema.

Questo comportamento solleva ulteriori interrogativi sulla natura e gli obiettivi del malware, poiché la manipolazione dei file di sistema potrebbe indicare un tentativo di compromettere l'integrità del sistema operativo o di installare componenti dannosi in posizioni critiche.

				Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Director
				Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Director
				Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Director
		C.\WINDOWS\system32\config	SUCCESS	Decired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Director
		C:\WINDOWS\system32\ntdl.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
		C:\WINDOWS\system32\kernel32.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
		C:\WINDOWS\system32\config\system	SHARING VIOLATION	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
		C:\WINDOWS\system32\unicode.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
		C:\WINDOWS\system32\locale.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
		C:\WINDOWS\system32\sortbls.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
		C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\MALWARE_U3_W2_L2.EXE	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
		C:\WINDOWS\system32\ctype.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
		C:\WINDOW5\system3Z\sortkey.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
		C:\WINDOWS\system32\apphalp.dll		Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
		C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
				Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
				Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
				Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
				Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
				Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
				Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
				Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-
				Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes
				Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes
				Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes
				Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes
				Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes
				Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes
				Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes
				Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes
				Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Directory, Sync
				Desired Access: Read Data/List Directory, Execute/Traverse, Read Attributes, Synchronize,
				Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous II
				Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous II
				Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-
				Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-
				Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Director
		C/		Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Director
				Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Director
		C:\WINDOWS\system32		Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Director
3372	CreateFile	C:\WINDOWS\system32\sychost.exe	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous II
	3377 2 33	3372 si CreateFile 3373 si CreateFile 3373 si CreateFile 3373 si CreateFile 3374 si CreateFile 3375 si CreateFile 3376 si CreateFile 3377 si CreateFile 3377 si CreateFile 3377 si CreateFile 3378 si CreateFile 3379 si CreateFile 3370 si CreateFile 3371 si CreateFile 3372 si CreateFile 3372 si CreateFile 3372 si CreateFile 3373 si CreateFile 3374 si CreateFile 3375 si CreateFile 3376 si CreateFile 3377 si CreateFile 3377 si CreateFile 3377 si CreateFile 3378 si CreateFile 3379 si CreateFile 3370 si CreateFile 3370 si CreateFile 3371 si CreateFile 3372 si CreateFile	Sincester File C.WMNDOWS Suptem 32 Sincester F	

Per ampliare la nostra comprensione delle tattiche impiegate dal malware, è rilevante evidenziare che, attraverso l'analisi con Process Explorer, è emerso che i processi utilizzati dal codice dannoso si camuffano sotto i nomi "explorer.exe" e "svchost.exe". Questa strategia è finalizzata a mimetizzarsi all'interno di processi legittimi del sistema operativo, rendendo così più arduo rilevare la sua esecuzione in background. Questa mascheratura rappresenta una sfida aggiuntiva per gli investigatori della sicurezza informatica, poiché richiede un'analisi più approfondita per individuare e contrastare l'attività del malware senza compromettere il funzionamento normale del sistema. Incorporando questa osservazione nella nostra analisi, possiamo concentrarci su metodi più sofisticati per rilevare e neutralizzare questa minaccia.

	<u> </u>					
	IEXPLORE.EXE		1,888 K	4,552 K	1588 Internet Explorer	Microsoft Corporation
-	IPROSetMonitor.exe		472 K	1,980 K	1692 Intel® PROSet Monitoring S	Intel Corporation
■ 🖳	explorer.exe		11,196 K	18,0 4 0 K	1700 Windows Explorer	Microsoft Corporation
	wmiprvse. exe		1,748 K	4,708 K	1732 WMI	Microsoft Corporation
	alg.exe		1,108 K	3,424 K	1736 Application Layer Gateway S.,	. Microsoft Corporation
	Wireshark.exe	1.56	95,536 K	16,160 K	1824	
	VGAuthService.exe		6,256 K	8,992 K	1836 VMware Guest Authenticatio	. VMware, Inc.
1	VBoxTray.exe		1,964 K	3,5 4 0 K	1848 VirtualBox Guest Additions Tr	. Oracle Corporation
	Procmon.exe		13,632 K	3,360 K	1976 Process Monitor	Sysinternals - www.sysinter
	sychostexe		864 K	2,264 K	3148 Generic Host Process for Wi	Microsoft Corporation
4	dumpcap.exe		1,928 K	4,644 K	3624 Dumpcap	The Wireshark developer
2	ргосекр.ехе		11,732 K	7,504 K	3824 Sysinternals Process Explorer	Sysinternals - www.sysinter
4	wuauchexe		5,556 K	5,060 K	3948 Automatic Updates	Microsoft Corporation
	DOM: NOT STORY			7775757575		



Per arricchire ulteriormente la nostra indagine, dopo l'analisi dinamica con Process Monitor, abbiamo eseguito un controllo aggiuntivo tramite Regshot.

Questo ci ha permesso di catturare e confrontare lo stato del Registro di sistema prima e dopo l'esecuzione del malware.

Attraverso questa procedura, possiamo identificare eventuali modifiche o aggiunte sospette al Registro di sistema, fornendo così un'ulteriore traccia per comprendere l'impatto e le intenzioni del malware. Integrando questo passaggio nel nostro processo di analisi, siamo in grado di ottenere una panoramica più completa delle azioni del malware e delle sue possibili implicazioni per la sicurezza del sistema.