



Ok

Time of Day Process Name	PID Operation	Path	Result	Detail
2:12:52:7349 Malware_U3_W2_L1.exe	216 - CreateFileMapping	C:\WINDOWS\system32Vaultrep.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE
1:12:52.7349 Malware_U3_W/2_L1.exe	216 RueryStandardInformationFile	C:\WINDOWS\system32\faultrep.dll	SUCCESS	Allocation/Size: 81,920, EndDIFile: 90,384, NumberOfLinks: 1, DeletePending: False, Directory: False
1:12:52.7419 Malware_U3_W2_L1.exe	216 - CreateFileMapping	C:\WINDOWS\system32Vaultrep.dll	SUCCESS	SyncType: SyncTypeOther
112.52.7413 Malware_U3_W2_L1.exe	216 🖳 CloseFile	C:\WINDOWS\system32Vaultrep.dll	SUCCESS	
	216 ReadFile	C:\WINDOWS\system32Vaultrep.dll	SUCCESS	Offset: 0, Length: 32,768,170 Flags: Non-cached, Paging I/O, Synchronous Paging I/O
1:12:52.7477 Malware_U3_W2_L1.exe	216 🖳 QueryOpen	C:\WINDOWS\system32Vaultep.dll	SUCCESS	CreationTime: 4/14/2008 4:41:54 AM, LastAccessTime: 2/6/2024 10:12:53 AM, LastWriteTime: 4/14/2008 4:41:54 AM, ChangeTime: 3/2
112:52:7556 Malware_U3_W2_L1.exe	216 KreateFile	C:\WINDOWS\system32Vaultrep.dll	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a,
112:52:7557 Malware_U3_W2_L1.exe	216 🖳 CreateFileMapping	C:\WINDOWS\system32\faultrep.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE
1:12:52.7557 Malware_U3_W2_L1.exe	216 RueryStandardInformationFile	C:\WINDOWS\system32Vaultrep.dll	SUCCESS	Allocation Size: 81,920, EndOfFile: 80,384, NumberOff, inks: 1, DeletePending: False, Directory: False
112:52:7557 Malware_U3_W2_L1.exe	216 🖳 CreateFileMapping	C:\WINDOWS\system32Vaultep.dll	SUCCESS	SyncType: SyncType@ther
1:12:52:7559 Malware_U3_W2_L1.exe	216 A CreateFileMapping	C:\WINDOWS\system32\faultrep.dll	SUCCESS	SyncType: SyncType(Ither
1:12:52:7561 Malware_U3_W2_L1.exe	216 🖳 CloseFile	C:\WINDOWS\system32Vaultep.dll	SUCCESS	
112:52:7669 Malware_U3_W2_L1.exe	216 🌉 Load Image	C:\WIND DWS\system32Vaultrep.dll	SUCCESS	Image Base: 0x69450000, Image Size: 0x16000
12.52.7669470.AM_alware_U3_W2_L1.exe	216 KeadFile	C: \WINDOWS\system32Vaultrep.dll	SUCCESS	Offset: 74.240, Length: 3,072,1/0 Flags: Non-cached, Paging I/O, Synchronous Paging I/O
112:52:7725 Malware_U3_W2_L1.exe	216 at Load Image	C:\WINDDWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x8000
12:52:7801 Malware_U3_W2_L1.exe	216 🥞 Load Image	C:\WINDOWS\system32\usererv:dll	SUCCESS	Image Base: 0x769c0000, Image Size: 0x04000
1:12:52:7803 Malware_U3_W2_L1.exe	216 QueryOpen	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\WINSTA.dll	NAME NOT FOUND	
1:12:52:7806 Malware_U3_W2_L1.exe	216 RueryOpen	C:\WINDOWS\system32\winsta.dll	SUCCESS	CreationTime: 4/14/2008 4:42:10 AM, LastAccessTime: 2/6/2024 10:12:31 AM, LastWriteTime: 4/14/2008 4:42:10 AM, ChangeTime: 3/5
3:12:52.7808 Malware_U3_W2_L1.exe	216 🖳 CreateFile	C:\WINDOWS\system32\winste.dll	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous ID Non-Alert, Non-Directory File, Attributes: n/a,
1:12:52:7886 Malware_U3_W2_L1.exe	216 KreateFileMapping	C:\WINDOWS\oystem32\winsta.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE
112.52.7887 Malware_U3_W2_L1.exe	216 🖳 CreateFileMapping	C:\WINDOWS\system32\winsta.dll	SUCCESS	SyncType: SyncTypeOther
3:12:52:7888 Malware_U3_W2_L1.exe	216 KCloseFile	C: \WIND D'WS\system32\winsta.dll	SUCCESS	
1:12:52.7891 Malware_U3_W2_L1.exe	216 💐 Load Image	C: \WINDOWS\system32\winsta.dll	SUCCESS	Image Base: 0x76360000, Image Size: 0x10000
112.52.7950 Malware_U3_W2_L1.exe	216 🌉 Load Image	C:\\wINDO\wS\\system32\netapi32.dl	SUCCESS	Image Base: 0x5b960000, Image Size: 0x55000
1:12:52:7951 Malware_U3_W2_L1.exe	216 QueryOpen	C: Documents and Settings:\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\WTSAPI32.dll	NAME NOT FOUND	
1:12:52:7953 Malware_U3_W2_L1.exe	216 QueryOpen	C:\WIND 0\WS\system32\wksapi32.dll	SUCCESS	CreationTime: 4/14/2008 4:42:12 AM, LastAccessTime: 2/6/2024 10:12:31 AM, LastWriteTime: 4/14/2008 4:42:12 AM, ChangeTime: 3/2
1:12:52:7954 Makvare_U3_W2_L1.exe	216 CreateFile	C:\WINDOWS\system32\wksapi32.dll	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a,
3:12:52:7997 Malware_U3_W/2_L1.exe	216 CreateFileMapping	C:\WINDOWS\system32\wksapi32.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE
1:12:52:7998 Malware_U3_W2_L1.exe	216 KreateFileMapping	C:\WINDOWS\system32\wtsapi32.dll	SUCCESS	SyncType: SyncType(Ither
0:12:52:7999 Malware_U3_W2_L1.exe	216 - CloseFile	C:\WINDOWS\system32\wksapi32.dll	SUCCESS	
3:12:52:8001 Malware_U3_W2_L1.exe	216 🌉 Load Image	C:\WINDBWS\system32\wtsapi32.dll	SUCCESS	Image Base: 0x76/50000, Image Size: 0x6000
1:12:52:8084 Makware_U3_W2_L1.exe	216 AQueryOpen	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_w2_L1\SETUPAPI.dll	NAME NOT FOUND	
112:52:8085 Malware_U3_W2_L1.exe	216 QueryOpen	C:\WINDEWS\system32\setupapi.dl	SUCCESS	CreationTime: 4/14/2008 4:42:06 AM, LastAccessTime: 2/6/2024 10:12:53 AM, LastWriteTime: 4/14/2008 4:42:06 AM, ChangeTime: 3/2
1:12:52:8087 Malware_U3_W2_L1.exe	216 CreateFile	C:\WINDOWS\oystem32\oetupapi.dl	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a,
112:52:8088 Malware_U3_W2_L1.exe	216 CreateFileMapping	C:\WINDOWS\system32\setupapi.dl	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE
1:12:52:9088 Malware_U3_W2_L1.exe	216 CreateFileMapping	C:\WINDOWS\system32\setupapi.dll	SUCCESS	SyncType: SyncTypeOther
112:52:8090 Malware_U3_W2_L1.exe 1:12:52:8178 Malware_U3_W2_L1.exe	216 K CloseFile	C:\WINDOWS\system32\setupapi.dl	SUCCESS	
312528178 Malware_U3_W2_L1.exe	216 at Load Image	C:\WINDDWS\system32\setupapi.dll	SUCCESS	Image Base: 0x77920000, Image Size: 0x/3000
112:52:8180 Malware_U3_W2_L1.exe	216 ReadFile	C:\WINDOWS\system32Vaultrep.dll	SUCCESS	Offset: 9.216, Length: 32,768, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
112:52:8217 Malware_U3_W2_L1.exe	216 ReadFile	C:\WINDDWS\system32\faultrep.dll	SUCCESS	Offset: 73,728, Length: 512, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
112:52:9005 Malware_U3_W2_L1.exe 1:12:52:9024 Malware_U3_W2_L1.exe	216 QueryOpen	C./WINDOWS	SUCCESS	CreationTime: 3/20/2017 9:34:22 PM, LastAccessTime: 2/6/2024 10:12:53 AM, LastWriteTime: 9/17/2022 6:29:50 PM, ChangeTime: 9/1
312.52.9024 Malware_U3_W2_L1.exe 312.52.9032 Malware_U3_W2_L1.exe	216 ReadFile	C:\WINDDWS\system32\faultrep.dll	SUCCESS	Offset: 41,984, Length: 31,744,1/0 Flags: Non-cached, Paging 1/0, Synchronous Paging 1/0
	216 ReadFile	C:\WINDOWS\system32Vaultrep.dll		Offset: 1,024, Length: 8,192, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
1:12:52:9153 Malware_U3_W2_L1.exe 1:12:52:9178 Malware_U3_W2_L1.exe	216 QueryOpen 216 CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Makware_U3_W2_L1.exe C:\Documents and Settings\Administrator	SUCCESS	CreationTime: 8/16/2022 1:37:31 PM, LastAccessTime: 2/6/2024 10:11:54 AM, LastWriteTime: 1/19/2011 10:10:41 AM, ChangeTime: 2/ Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous ID Non-Alet, Attributes: n/a, SI
0:12:52:9178 Malware_U3_W2_L1.exe 0:12:52:9179 Malware_U3_W2_L1.exe	216 QueryDirectory	C: VD ocuments and Settings \Administrator\Desktop C: \Documents and Settings \Administrator	SUCCESS	Filter: Desktop, 1: Desktop, FileInformationClass: FileBothDirectoryInformation
112.52.9179 Malware_U3_W2_L1.exe 1.12.52.9237 Malware_U3_W2_L1.exe	216 - CloseFile		SUCCESS	1000 P. C.
112525237 Maiware_U3_W2_L1.exe 112529272 Maiware_U3_W2_L1.exe	216 T Load Image 216 CreateFile	C:\WINDOWS\system32\shel32.dll C:\WINDOWS\system32\shel32.dll	SUCCESS	Image Basic 0x7c9c0000. Image Size: 0x817000 Desired Access: Generic Read/Execute. Disposition: Open. Options: Synchronous IO Non-Alert. Non-Directory File. Attributes: n/a, ShareM
112523272 Maware_U3_W2_L1.exe				
112:52:9311 Malware_U3_W2_L1.exe	216 CreateFileMapping	C:\WINDOWS\system32\shell32.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READONLY
112:52:9311 Malware_U3_W2_L1.exe 1:12:52:9312 Malware_U3_W2_L1.exe	216 QueryStandardInformationFile	C:\WINDOWS\system32\sheli32.dll C:\WINDOWS\system32\sheli32.dll	SUCCESS	AllocationSize: 8,462,336, EndOfFile: 8,461,312, NumberOfLinks: 1, DeletePending: False, Directory: False
	216 ScreateFileMapping	L:\winduws\systemsz\snetsz.dt	SULLESS	SyncType: SyncTypeOther

Annulla

Aiuto

