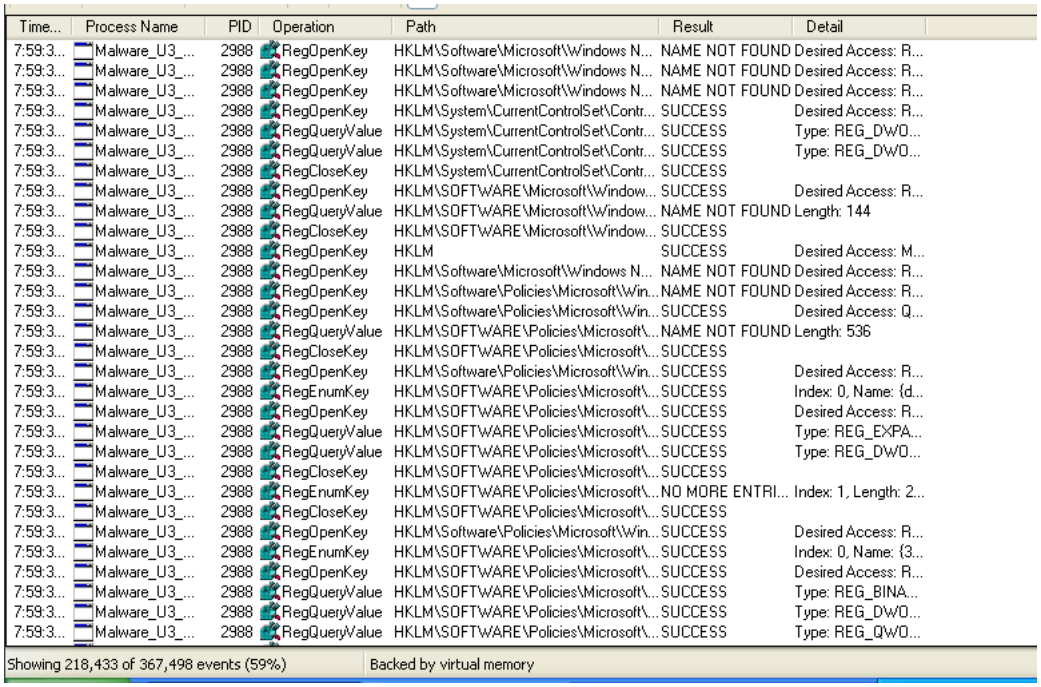
Dopo aver analizzato il file eseguibile Esercizio_Pratico_U3_W2_L2 ho visto che innanzitutto apriva una richiesta di aperture di terminal server così da fornire un accesso remoto e successivamente fà molte richieste di apertura registro e successivamente di Dword e Qword su vari path questo mi fa ipotizzare che si tratti di uno spyware che sta cercando si raccogliere info sulla nostra macchina.



Time...	Process Name	PID	Operation	Path	Result	Detail
7:59:3...	Malware_U3_...	2988	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: R...
7:59:3...	Malware_U3_...	2988	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: R...
7:59:3...	Malware_U3_...	2988	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: R...
7:59:3...	Malware_U3_...	2988	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
7:59:3...	Malware_U3_...	2988	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWO...
7:59:3...	Malware_U3_...	2988	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWO...
7:59:3...	Malware_U3_...	2988	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
7:59:3...	Malware_U3_...	2988	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...
7:59:3...	Malware_U3_...	2988	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 144
7:59:3...	Malware_U3_...	2988	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
7:59:3...	Malware_U3_...	2988	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
7:59:3...	Malware_U3_...	2988	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: R...
7:59:3...	Malware_U3_...	2988	RegOpenKey	HKLM\Software\Policies\Microsoft\Win...	NAME NOT FOUND	Desired Access: R...
7:59:3...	Malware_U3_...	2988	RegOpenKey	HKLM\Software\Policies\Microsoft\Win...	SUCCESS	Desired Access: Q...
7:59:3...	Malware_U3_...	2988	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Length: 536
7:59:3...	Malware_U3_...	2988	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
7:59:3...	Malware_U3_...	2988	RegOpenKey	HKLM\Software\Policies\Microsoft\Win...	SUCCESS	Desired Access: R...
7:59:3...	Malware_U3_...	2988	RegEnumKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Index: 0, Name: {d...
7:59:3...	Malware_U3_...	2988	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Desired Access: R...
7:59:3...	Malware_U3_...	2988	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Type: REG_EXPA...
7:59:3...	Malware_U3_...	2988	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Type: REG_DWO...
7:59:3...	Malware_U3_...	2988	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
7:59:3...	Malware_U3_...	2988	RegEnumKey	HKLM\SOFTWARE\Policies\Microsoft\...	NO MORE ENTRI...	Index: 1, Length: 2...
7:59:3...	Malware_U3_...	2988	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
7:59:3...	Malware_U3_...	2988	RegOpenKey	HKLM\Software\Policies\Microsoft\Win...	SUCCESS	Desired Access: R...
7:59:3...	Malware_U3_...	2988	RegEnumKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Index: 0, Name: {3...
7:59:3...	Malware_U3_...	2988	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Desired Access: R...
7:59:3...	Malware_U3_...	2988	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Type: REG_BINA...
7:59:3...	Malware_U3_...	2988	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Type: REG_DWO...
7:59:3...	Malware_U3_...	2988	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Type: REG_QWO...

Showing 218,433 of 367,498 events (59%) Backed by virtual memory