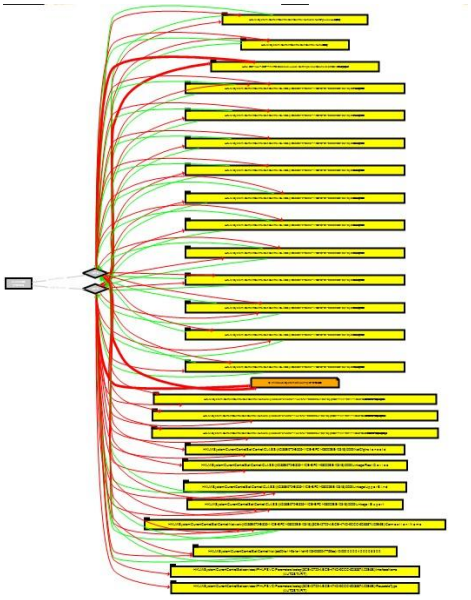
Malware Analysis 2

Analisi Malware pt2:

- Avvio procmon.exe e inizio cattura
- Avvio malware
- Stop cattura
- Analisi
- Import su ProcDOT

Praticamente crea un processo svchost.exe e si killa poi svchosts fa una serie di modifiche al registro di sistema e poi si killa.



Qui sotto l'analisi su procmon

Time ...	Process Name	PID	Operation	Path	Result	Detail	TID
12:24:...	Malware_U3_...	432	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys	1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Read	1176
12:24:...	Malware_U3_...	432	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS		1176
12:24:40.4379835 PM	Malware_U3_...	432	RegOpenKey	HKLM\Software\Wow6432Node\Micro...	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys	1176
12:24:...	Malware_U3_...	432	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Read	1176
12:24:...	Malware_U3_...	432	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	1176
12:24:...	Malware_U3_...	432	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS		1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Read	1176
12:24:...	Malware_U3_...	432	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	1176
12:24:...	Malware_U3_...	432	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0	1176
12:24:...	Malware_U3_...	432	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS		1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Desired Access: Query Value	1176
12:24:...	Malware_U3_...	432	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	1176
12:24:...	Malware_U3_...	432	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS		1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Read	1176
12:24:...	Malware_U3_...	432	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	1176
12:24:...	Malware_U3_...	432	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Length: 36, Data: 00060101.00060101	1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Query Value	1176
12:24:...	Malware_U3_...	432	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Desired Access: Query Value	1176
12:24:...	Malware_U3_...	432	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	1176
12:24:...	Malware_U3_...	432	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0	1176
12:24:...	Malware_U3_...	432	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS		1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: Query Value	1176
12:24:...	Malware_U3_...	432	RegSetInfoKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	1176
12:24:...	Malware_U3_...	432	RegQueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_SZ, Length: 142, Data: C:\Users\user\AppData\Local\Microsoft\Window...	1176
12:24:...	Malware_U3_...	432	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS		1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Query Value	1176
12:24:...	Malware_U3_...	432	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Read	1176
12:24:...	Malware_U3_...	432	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	1176
12:24:...	Malware_U3_...	432	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS		1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Read	1176
12:24:...	Malware_U3_...	432	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	1176
12:24:...	Malware_U3_...	432	RegEnumKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Index: 0, Name: en-US	1176
12:24:...	Malware_U3_...	432	RegQueryKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Query: HandleTags, HandleTags: 0x400	1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Read	1176
12:24:...	Malware_U3_...	432	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 145	1176
12:24:...	Malware_U3_...	432	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS		1176
12:24:...	Malware_U3_...	432	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS		1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKCU	SUCCESS	Desired Access: Maximum Allowed, Granted Access: All Access	1176
12:24:...	Malware_U3_...	432	RegQueryKey	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0	1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Read	1176
12:24:...	Malware_U3_...	432	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	1176
12:24:...	Malware_U3_...	432	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS		1176
12:24:...	Malware_U3_...	432	RegCloseKey	HKCU	SUCCESS		1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKCU	SUCCESS	Desired Access: Maximum Allowed, Granted Access: All Access	1176
12:24:...	Malware_U3_...	432	RegQueryKey	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0	1176
12:24:...	Malware_U3_...	432	RegQueryKey	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0	1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKCU\Control Panel\Desktop\Languag...	SUCCESS	Desired Access: Read	1176
12:24:...	Malware_U3_...	432	RegSetInfoKey	HKCU\Control Panel\Desktop\Languag...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	1176
12:24:...	Malware_U3_...	432	RegCloseKey	HKCU\Control Panel\Desktop\Languag...	SUCCESS		1176
12:24:...	Malware_U3_...	432	RegCloseKey	HKCU	SUCCESS		1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKCU	SUCCESS	Desired Access: Maximum Allowed, Granted Access: All Access	1176
12:24:...	Malware_U3_...	432	RegQueryKey	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0	1176
12:24:...	Malware_U3_...	432	RegQueryKey	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0	1176
12:24:...	Malware_U3_...	432	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: Read	1176