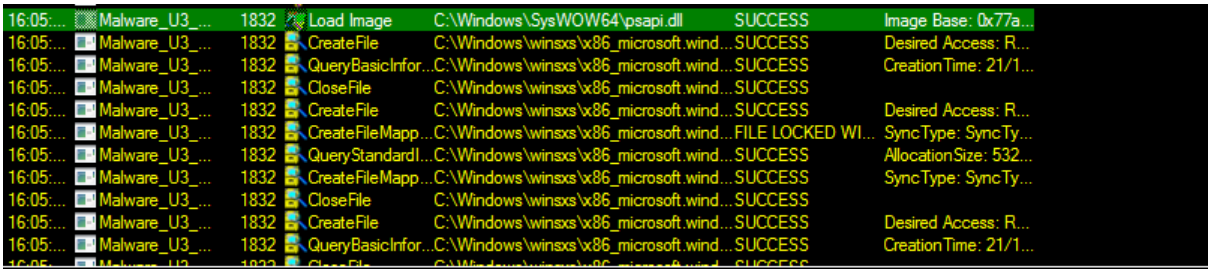
S10L2

Analisi dinamica

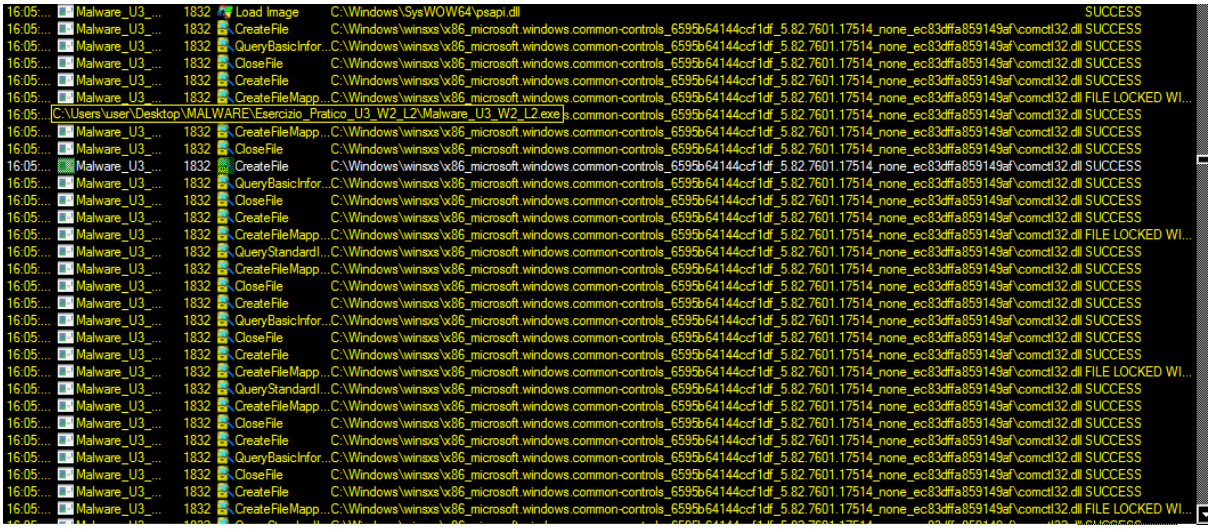
Identificare eventuali azioni del malware sul file system utilizzando ProcessMonitor (procmon) ,Identificare eventuali azioni del malware su processi e thread utilizzando ProcessMonitor.

SOLUZIONE

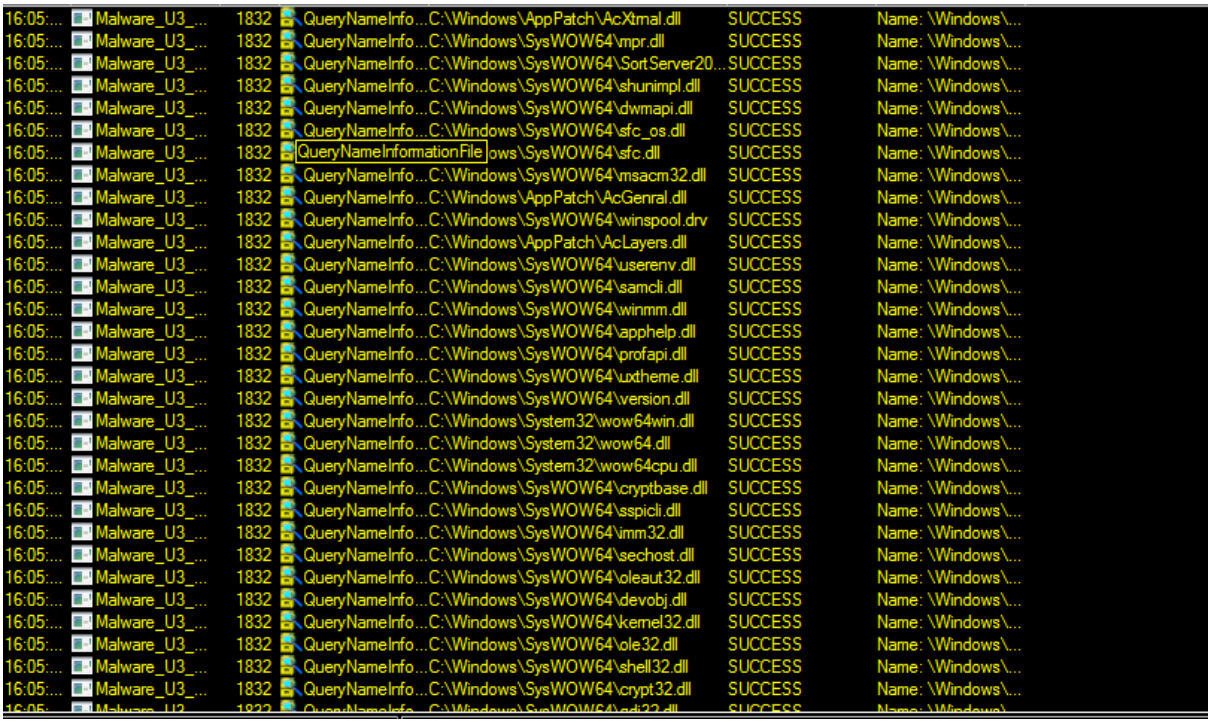
Come prima cosa mettiamo la nostra macchina in sicurezza quindi,eliminiamo la connessione e eventuali cartelle condivise,una volta fatto ciò procediamo ad analizzare il malware in questione.



Possiamo notare che il malware carica una libreria (psapi.dll) la quale fornisce funzioni per ottenere informazioni sui processi e sui moduli in esecuzione nel sistema,quindi sta cercando di raccogliere informazioni.



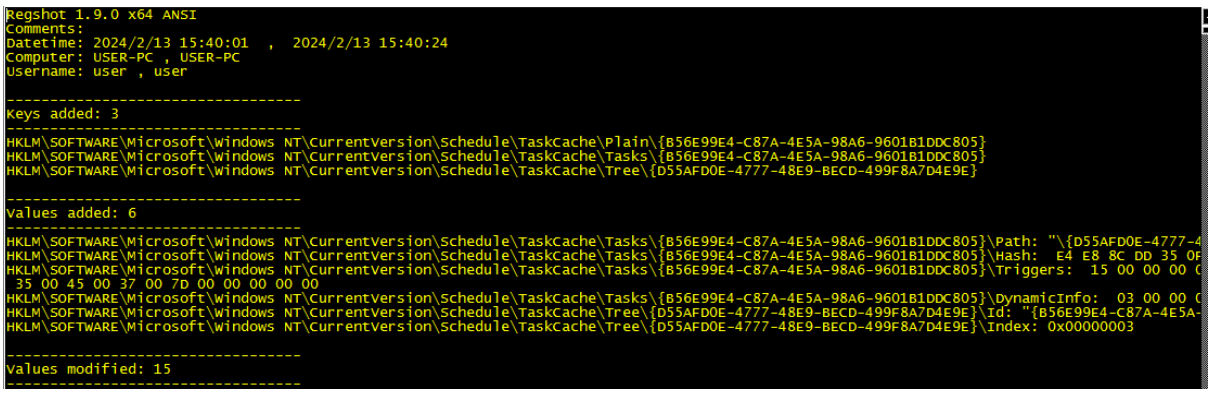
Dopodichè va a modificare la libreria ‘comctl32.dll’ per eseguire il proprio codice e inoltre invoca anche la libreria ‘acgenral.dll’ per eludere le misure di sicurezza.



16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\AppPatch\AcXtrnal.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\mpr.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\SortServer20...	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\shunimpl.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\sfc_os.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInformationFile	ows\SysWOW64\sfc.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\msacm32.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\AppPatch\AcGenral.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\winspool.drv	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\AppPatch\AcLayers.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\userenv.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\samcli.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\winmm.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\profapi.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\uxtheme.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\version.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\System32\wow64win.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\System32\wow64.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\System32\wow64cpu.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\sspicli.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\devobj.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Name: \Windows\...
16:05:...	Malware_U3_...	1832	QueryNameInfo...	C:\Windows\SysWOW64\crypt32.dll	SUCCESS	Name: \Windows\...

Una volta che ha completato queste operazioni,il malware va a ottenere informazioni su varie librerie e si posiziona in una cartella di sistema in modo tale da avviarsi ogni volta che noi accendiamo il pc.

Regshot



```
Regshot 1.9.0 x64 ANSI
Comments:
Datetime: 2024/2/13 15:40:01   ,   2024/2/13 15:40:24
Computer: USER-PC , USER-PC
Username: user , user

----------------------------------
Keys added: 3
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Plain\{B56E99E4-C87A-4E5A-98A6-9601B1DDC805}
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{B56E99E4-C87A-4E5A-98A6-9601B1DDC805}
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\{D55AFD0E-4777-48E9-BECD-499F8A7D4E9E}

----------------------------------
Values added: 6
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{B56E99E4-C87A-4E5A-98A6-9601B1DDC805}\Path: "\{D55AFD0E-4777-4
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{B56E99E4-C87A-4E5A-98A6-9601B1DDC805}\Hash:  E4 E8 8C DD 35 0F
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{B56E99E4-C87A-4E5A-98A6-9601B1DDC805}\Triggers:  15 00 00 00 0
 35 00 45 00 37 00 7D 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{B56E99E4-C87A-4E5A-98A6-9601B1DDC805}\DynamicInfo:  03 00 00 0
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\{D55AFD0E-4777-48E9-BECD-499F8A7D4E9E}\Id: "{B56E99E4-C87A-4E5A-
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\{D55AFD0E-4777-48E9-BECD-499F8A7D4E9E}\Index: 0x00000003

----------------------------------
Values modified: 15
----------------------------------
```

Attraverso un tool chiamato *regshot* andiamo a effettuare un’istantanea delle modifiche fatte dal malware una volta eseguito, e come possiamo notare ha effettuato 15 modifiche al sistema.

Considerazioni finali

Il malware in questione è un keylogger perchè va a modificare comctl32.dll, la quale intercetta l'input dell'utente.Mentre psapi.dll importata dal malware va a identificare in quali finestre si verificano gli inserimenti da tastiera e inoltre va a fare una scalata dei privilegi inserendosi all'interno di una directory di sistema in modo tale da avviarsi all'avvio del pc.