

# MALWARE U3 W2 L2 Analisi con Procmon:

Il malware fa le seguenti azioni in specifico interessanti:

```
HKLM\SOFTWARE\POLICIES\MICROSOFT\W  
C:\WINDOWS\system32\advapi32.dll  
C:\WINDOWS\system32\rpcrt4.dll  
C:\WINDOWS\system32\secur32.dll
```

Chiama queste 3 DLL, che secondo chatgpt

Un malware potrebbe chiamare le DLL advapi32.dll, rpcrt4.dll e secur32.dll per vari scopi malevoli. Ecco una descrizione dei motivi per cui un malware potrebbe utilizzare ciascuna di queste DLL:

## 1. advapi32.dll

Questa DLL fornisce numerose funzioni legate alla sicurezza e alla gestione del sistema, che possono essere sfruttate da un malware per:

- **Elevazione dei Privilegi:** Un malware potrebbe utilizzare le funzioni di gestione degli account utente e dei permessi per ottenere privilegi più elevati.
- **Manipolazione del Registro di Sistema:** Il malware potrebbe accedere e modificare il Registro di sistema per persistere nel sistema, eseguire payload all'avvio o modificare impostazioni di sicurezza.
- **Servizi di Windows:** Un malware potrebbe gestire i servizi di Windows, avviarli, fermarli o modificarli per camuffarsi o garantire la propria esecuzione.
- **Crittografia:** Utilizzare le funzioni di crittografia per cifrare i dati rubati o per eseguire attacchi ransomware.

## 2. rpcrt4.dll

Questa DLL gestisce le chiamate di procedura remota (RPC), che possono essere sfruttate da un malware per:

- **Comunicazioni Remota:** Stabilire comunicazioni con server di comando e controllo (C2) per ricevere istruzioni o esfiltrare dati.
- **Attacchi Distribuiti:** Coordinare azioni malevole su più macchine in una rete, come parte di un attacco distribuito.
- **Evasione delle Difese:** Utilizzare RPC per eseguire operazioni in un contesto di sicurezza differente, aggirando alcune misure di sicurezza locali.

## 3. secur32.dll

Questa DLL è legata all'autenticazione e alla sicurezza di rete, e può essere utilizzata da un malware per:

- **Autenticazione Falsa:** Inviare credenziali di autenticazione false o intercettare credenziali legittime per accedere a risorse di rete.
- **Sfruttamento di Protocolli di Sicurezza:** Manipolare protocolli di sicurezza come Kerberos o NTLM per ottenere accesso non autorizzato a sistemi e dati.
- **Esecuzione di Attacchi Man-in-the-Middle (MitM):** Posizionarsi tra due punti di comunicazione per intercettare e manipolare il traffico di rete.

## Esempi di Attività Malevole

- **Keylogging e Esfiltrazione di Credenziali:** Un malware potrebbe utilizzare secur32.dll per catturare credenziali di accesso e poi inviarle tramite rpcrt4.dll a un server remoto.
- **Persistenza e Manipolazione del Sistema:** Utilizzando advapi32.dll, un malware potrebbe modificare le chiavi di registro e i servizi di sistema per assicurarsi che venga eseguito ad ogni avvio del sistema.
- **Attacchi Coordinati in Rete:** Utilizzando rpcrt4.dll, un malware potrebbe eseguire comandi su più macchine nella rete per diffondere ulteriormente l'infezione o coordinare un attacco distribuito.

Il malware crea persistenza immettendosi in “Prefetch” di windows.

:25:37.22776...	Malware_U3_W2_L2.exe	1152	Thread Create			SUCCESS	Thread ID: 1476
:25:37.22832...	Malware_U3_W2_L2.exe	1152	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe		SUCCESS	Name: \Docum...
:25:37.22886...	Malware_U3_W2_L2.exe	1152	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe		SUCCESS	Image Base: 0x...
:25:37.22907...	Malware_U3_W2_L2.exe	1152	Load Image	C:\WINDOWS\system32\ntdll.dll		SUCCESS	Image Base: 0x...
:25:37.22910...	Malware_U3_W2_L2.exe	1152	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe		SUCCESS	Name: \Docum...
:25:37.22933...	Malware_U3_W2_L2.exe	1152	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf		SUCCESS	Desired Access:...
:25:37.22950...	Malware_U3_W2_L2.exe	1152	QueryStandardInformation...	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf		SUCCESS	AllocationSize: 8...
:25:37.22965...	Malware_U3_W2_L2.exe	1152	ReadFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf		SUCCESS	Offset: 0, Lengt...
:25:37.23234...	Malware_U3_W2_L2.exe	1152	CloseFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf		SUCCESS	
:25:37.23242...	Malware_U3_W2_L2.exe	1152	CreateFile	C:\		SUCCESS	Desired Access:...
:25:37.23245...	Malware_U3_W2_L2.exe	1152	QueryInformationVolume	C:\		SUCCESS	VolumeCreation...
:25:37.23249...	Malware_U3_W2_L2.exe	1152	FileSystemControl	C:\		SUCCESS	Control: FSCTL...
:25:37.23320...	Malware_U3_W2_L2.exe	1152	CreateFile	C:\		SUCCESS	Desired Access:...

Il malware si nasconde avviandosi come “svchost.exe”

1:25:37.29970...	Malware_U3_W2_L2.exe	1152	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\CodeIdentifiers\LogfileName			
1:25:37.29972...	Malware_U3_W2_L2.exe	1152	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\CodeIdentifiers			
1:25:37.29973...	Malware_U3_W2_L2.exe	1152	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option			
1:25:37.29978...	Malware_U3_W2_L2.exe	1152	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\svchost.exe			
1:25:37.30004...	Malware_U3_W2_L2.exe	1152	CreateFile	C:\WINDOWS\system32\svchost.exe.Manifest			
1:25:37.30051...	Malware_U3_W2_L2.exe	1152	Process Create	C:\WINDOWS\system32\svchost.exe			
1:25:37.30078...	Malware_U3_W2_L2.exe	1152	CloseFile	C:\WINDOWS\system32\svchost.exe			
1:25:37.30081...	Malware_U3_W2_L2.exe	1152	IRP_MJ_CLOSE	C:\WINDOWS\system32\svchost.exe			
1:25:37.98731...	Malware_U3_W2_L2.exe	1152	Process Profiling				

## Conclusione:

Il malware Malware\_U3\_W2\_L2.exe sembra essere un eseguibile che si avvia e termina rapidamente, caricando vari moduli di sistema nel processo. Questo comportamento può indicare che il malware esegue una serie di operazioni rapidamente, probabilmente per evitare il rilevamento. I moduli caricati suggeriscono che potrebbe avere funzionalità legate alla manipolazione delle autenticazioni di sicurezza o alla comunicazione di rete.