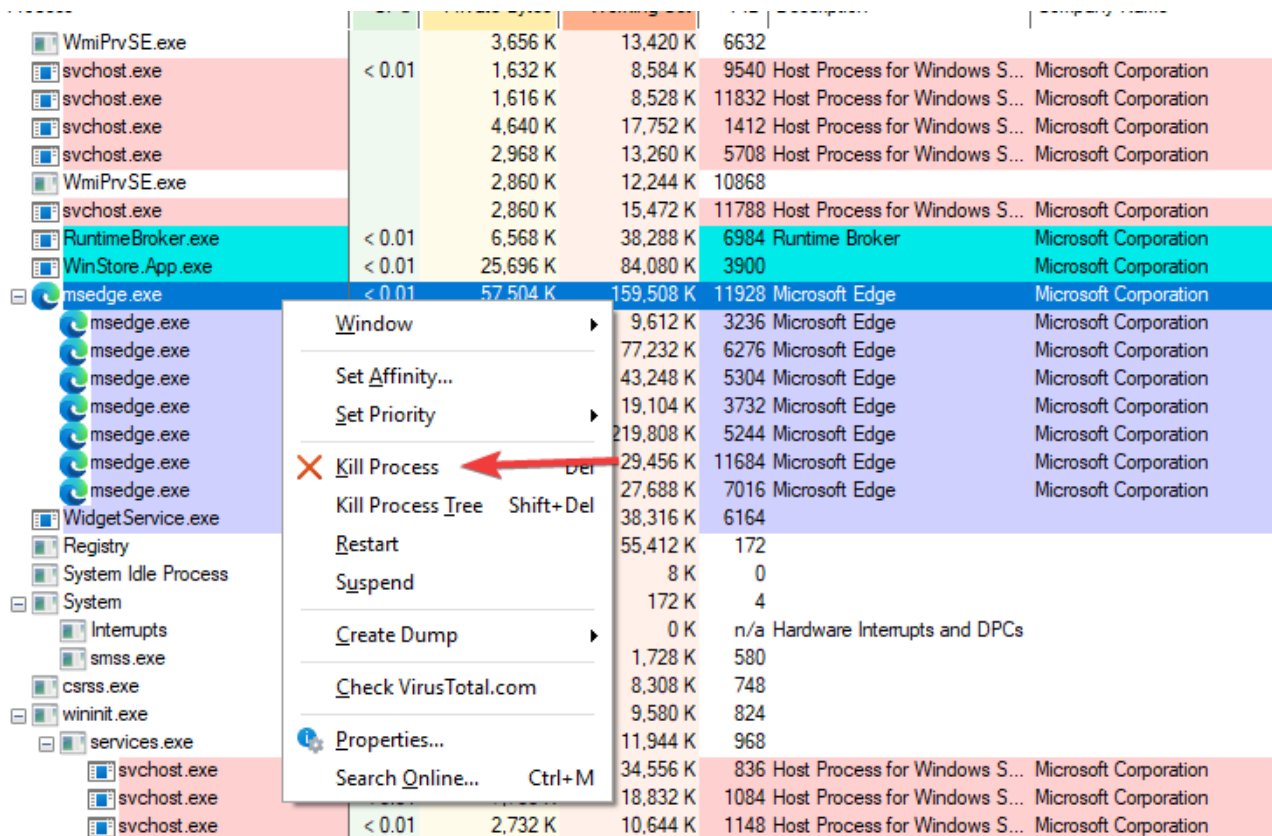


S11L1

UNIT 3

Marco Falchi



WmiPrvSE.exe		3,656 K	13,420 K	6632		
svchost.exe	< 0.01	1,632 K	8,584 K	9540	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,616 K	8,528 K	11832	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,640 K	17,752 K	1412	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,968 K	13,260 K	5708	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		2,860 K	12,244 K	10868		
svchost.exe		2,860 K	15,472 K	11788	Host Process for Windows S...	Microsoft Corporation
RuntimeBroker.exe	< 0.01	6,568 K	38,288 K	6984	Runtime Broker	Microsoft Corporation
WinStore.App.exe	< 0.01	25,696 K	84,080 K	3900		Microsoft Corporation
msedge.exe	< 0.01	57,504 K	159,508 K	11928	Microsoft Edge	Microsoft Corporation
msedge.exe			9,612 K	3236	Microsoft Edge	Microsoft Corporation
msedge.exe			77,232 K	6276	Microsoft Edge	Microsoft Corporation
msedge.exe			43,248 K	5304	Microsoft Edge	Microsoft Corporation
msedge.exe			19,104 K	3732	Microsoft Edge	Microsoft Corporation
msedge.exe			219,808 K	5244	Microsoft Edge	Microsoft Corporation
msedge.exe			29,456 K	11684	Microsoft Edge	Microsoft Corporation
msedge.exe			27,688 K	7016	Microsoft Edge	Microsoft Corporation
WidgetService.exe			38,316 K	6164		
Registry			55,412 K	172		
System Idle Process			8 K	0		
System			172 K	4		
Interrupts			0 K	n/a	Hardware Interrupts and DPCs	
smss.exe			1,728 K	580		
csrss.exe			8,308 K	748		
wininit.exe			9,580 K	824		
services.exe			11,944 K	968		
svchost.exe			34,556 K	836	Host Process for Windows S...	Microsoft Corporation
svchost.exe			18,832 K	1084	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	2,732 K	10,644 K	1148	Host Process for Windows S...	Microsoft Corporation

Cosa è successo alla finestra del browser web quando il processo è stato terminato?

Il processo si è chiuso chiudendo quindi il browser web.

Cosa è successo durante il processo ping?

Durante il ping il “sottoprocesso” cambia nome da conhost.exe a PING.EXE

The screenshot shows Process Explorer with a list of running processes. A red arrow points to the 'conhost.exe' process, which is the parent of 'PING.EXE'. Below the Process Explorer window, a Command Prompt window shows the execution of the 'ping 8.8.8.8' command, displaying successful replies.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		4,564 K	20,948 K	1236	Host Process for Windows S...	Microsoft Corporation
explorer.exe	< 0.01	98,316 K	260,220 K	4456	Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		1,844 K	13,000 K	628	Windows Security notificatio...	Microsoft Corporation
VBBoxTray.exe	< 0.01	2,736 K	14,548 K	8256	VirtualBox Guest Additions Tr...	Oracle and/or its affiliates
OneDrive.exe		44,076 K	124,632 K	7236	Microsoft OneDrive	Microsoft Corporation
procexp.exe	0.38	24,064 K	53,904 K	5948	Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe		2,220 K	5,872 K	4844		
conhost.exe	< 0.01	8,152 K	27,888 K	11916		
PING.EXE	< 0.01	952 K	5,324 K	9200		
svchost.exe		2,424 K	15,540 K	5172	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,952 K	12,152 K	5488	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,036 K	26,356 K	5792	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,648 K	8,596 K	5912	Host Process for Windows S...	Microsoft Corporation
svchost.exe		8,388 K	30,516 K	5940	Host Process for Windows S...	Microsoft Corporation
SearchHost.exe	< 0.01	51,980 K	140,816 K	6452		Microsoft Corporation
msedgewebview2.exe		38,004 K	123,032 K	5432	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		2,196 K	9,096 K	5000	Microsoft Edge WebView2	Microsoft Corporation

```
Administrator: Command Prompt - ping 8.8.8.8

C:\Windows\System32>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=32ms TTL=255
Reply from 8.8.8.8: bytes=32 time=32ms TTL=255
Reply from 8.8.8.8: bytes=32 time=31ms TTL=255
```

Cosa è successo al processo figlio conhost.exe?

Se il comando Kill process viene fatto al processo figlio si chiude anche il processo padre durante la mansione precedente effutiamo una scansione di virus tramite virustotal.

The screenshot shows the VirusTotal interface for a file named CONHOST.EXE. The file is identified as 'peexe' and is marked as 'known-distributor'. The scan results show that no security vendors flagged this file as malicious.

Community Score: 0 / 71

No security vendors flagged this file as malicious

29e4840bf10bafb9fd5bcad70612a19b78a4a89b8f30220edc654bd49832d916

CONHOST.EXE

Size: 984.00 KB

Last Analysis Date: 4 hours ago

peexe known-distributor 64bits detect-debug-environment idle

Che tipo di informazioni sono disponibili nella finestra Proprietà? (ia)

TCP/IP: Questa scheda mostra le informazioni relative alla rete, come le connessioni TCP (Transmission Control Protocol) e IP (Internet Protocol) attive, inclusi i numeri di porta e gli indirizzi remoti usati dal processo conhost.exe. Aiuta a monitorare l'attività di rete.

Security: La scheda Security mostra i permessi di utente e di gruppo per il processo. Questo determina chi può eseguire, modificare o terminare il processo. È una parte cruciale del controllo degli accessi e della sicurezza del sistema.

Environment: Questa sezione mostra le variabili d'ambiente associate al processo. Le variabili d'ambiente sono valori dinamici che possono influenzare il modo in cui un processo viene eseguito. Ad esempio, la variabile PATH indica al sistema dove cercare i file eseguibili.

Strings: Questa scheda ti permette di visualizzare le stringhe di testo incorporate nel file eseguibile. Queste stringhe possono includere percorsi di file, nomi di funzioni, messaggi di errore e informazioni sulla versione, utili per il debug e il reverse engineering.

Image: La scheda Image fornisce informazioni generali sul file eseguibile stesso, come la sua posizione sul disco, la dimensione, la data di creazione e il numero di versione. Spesso è la visualizzazione predefinita quando apri le proprietà.

Performance e Performance Graph: Queste schede vengono usate per monitorare l'utilizzo delle risorse del processo. Performance mostra l'utilizzo attuale delle risorse in un formato di elenco (ad esempio, utilizzo di CPU, memoria, disco e GPU), mentre Performance Graph presenta questi dati in un grafico in tempo reale per una visualizzazione più semplice dei trend e dei picchi.

GPU Graph: Questa scheda si concentra specificamente sull'utilizzo della GPU (Graphics Processing Unit) da parte del processo. Mostra quanto il processo sta usando la scheda grafica per il rendering o altre attività, il che è particolarmente rilevante per le applicazioni con un'interfaccia utente grafica.

Threads: La scheda Threads elenca i singoli thread di esecuzione che girano all'interno del processo. Un processo può avere più thread per eseguire compiti diversi contemporaneamente, e questa scheda fornisce dettagli su ciascuno di essi, come il suo ID e lo stato.

Esaminare gli handle. A cosa puntano gli handle?

La colonna name indica il percorso o il nome del file a cui ha accesso il processo mentre la colonna Type indica il tipo di file.

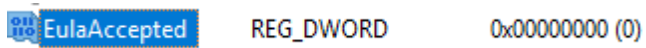
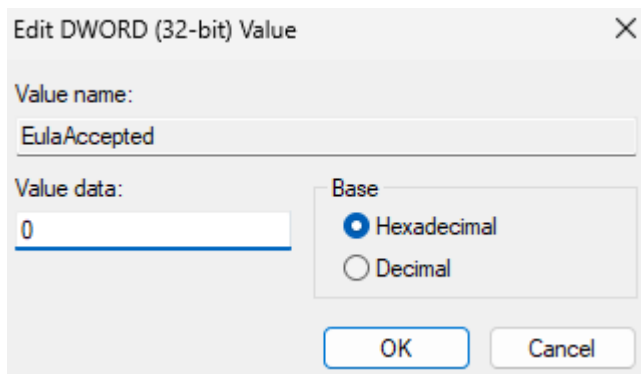
File: Puntano a file e cartelle aperti sul disco rigido.
Key: Puntano a chiavi del Registro di sistema .
Semaphore: Puntano a semafori , un meccanismo di sincronizzazione usato per controllare l'accesso a una risorsa condivisa.
Mutant: Puntano a mutex , un altro meccanismo di sincronizzazione che fornisce accesso esclusivo a una risorsa.
Thread: Puntano a thread di esecuzione all'interno del processo. I numeri 12192, 2928 e 1228 sono gli ID dei thread.
Section: Puntano a sezioni (o sezioni di memoria mappate a file). Queste sono aree di memoria condivisa che consentono a due o più processi di comunicare o di condividere dati.
Window Station: Puntano alle stazioni finestra , che sono ambienti di lavoro sicuri che contengono desktop, appunti e altri oggetti correlati all'interfaccia utente.
Event: Puntano a eventi , un meccanismo di sincronizzazione per notificare a un thread il verificarsi di un evento.
Directory: Puntano a directory di oggetti , che sono spazi dei nomi usati dal kernel per organizzare gli oggetti.

Type	Name
ALPC Port	\RPC Control\OLEBD0D98296B5C103828E754AE4D0A
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
File	\Device\ConDrv
File	C:\Windows
File	C:\Windows\System32\en-US\Conhost.exe.mui
File	\Device\NamedPipe\
File	\Device\CNG
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKCU
Key	HKLM
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Ole
Key	HKCU\Software\Classes\Local Settings\Software\Microsoft
Key	HKCU\Software\Classes\Local Settings
Key	HKCU\Software\Classes
Key	HKCR\PackagedCom
Key	HKCR\PackagedCom\ClassIndex
Key	HKCU\Software\Classes\PackagedCom
Key	HKCU\Software\Classes\PackagedCom\Package
Key	HKCR\PackagedCom\Package
Key	HKCU\Software\Classes
Key	HKCU\Software\Classes
Key	HKCR\PackagedCom\InterfaceIndex
Mutant	\Sessions\1\BaseNamedObjects\SM0:12280:304:WilStaging_02
Mutant	\Sessions\1\BaseNamedObjects\SM0:12280:120:WilError_03
Section	\BaseNamedObjects__ComCatalogCache__
Section	\BaseNamedObjects__ComCatalogCache__
Semaphore	\Sessions\1\BaseNamedObjects\SM0:12280:304:WilStaging_02_p0
Semaphore	\Sessions\1\BaseNamedObjects\SM0:12280:304:WilStaging_02_p0h
Semaphore	\Sessions\1\BaseNamedObjects\SM0:12280:120:WilError_03_p0
Semaphore	\Sessions\1\BaseNamedObjects\SM0:12280:120:WilError_03_p0h
Thread	conhost.exe(12280): 12192
Thread	conhost.exe(12280): 2928
Thread	conhost.exe(12280): 2928
Thread	conhost.exe(12280): 1228
WindowStation	\Sessions\1\Windows\WindowStations\WinSta0
WindowStation	\Sessions\1\Windows\WindowStations\WinSta0

Qual è il valore per questa chiave di registro nella colonna Dati (Data)?

Dopo aver cambiato il valore da 1 a 0 il valore diventa 0x00000000 (0)

Computer\HKEY_CURRENT_USER\Software\Sysinternals\Process Explorer			
	Name	Type	Data
> Control Panel	ETWstandardUs...	REG_DWORD	0x00000000 (0)
> Environment	EulaAccepted	REG_DWORD	0x00000001 (1)
> EUDC	FindWindowpla...	REG_BINARY	2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00...
> Keyboard Layout	FormatIoBvtes	REG_DWORD	0x00000001 (1)
> Microsoft			



Quando apri Process Explorer, cosa vedi?

Noto che il valore ritorna in automatico a 1 poiché è come se rifirmasse il contratto EULA portando quindi nuovamente il valore al suo stato iniziale