

Progetto S11/L5

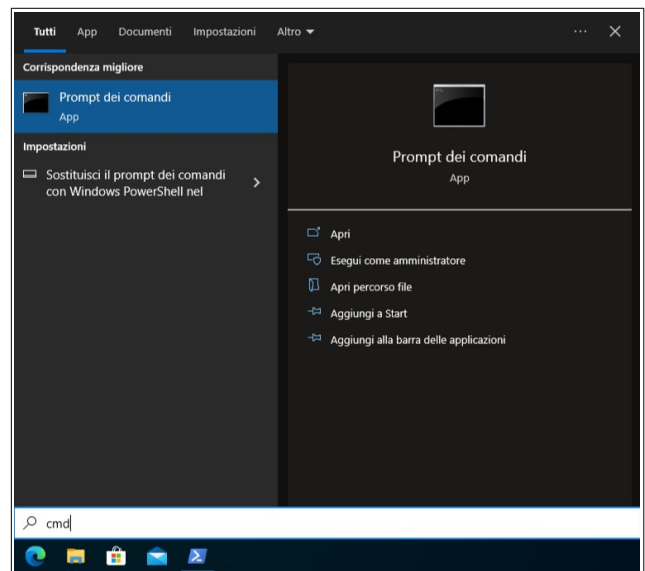
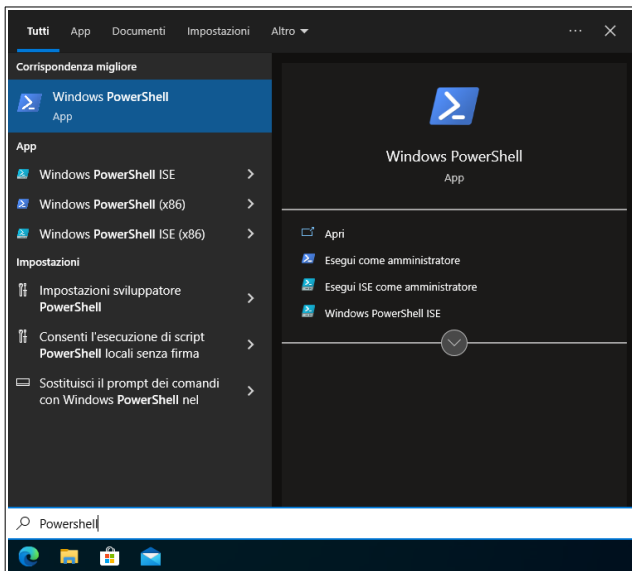
Utilizzo di PowerShell

Introduzione

L'obiettivo di questo esercizio è stato esplorare le funzionalità di Windows PowerShell.

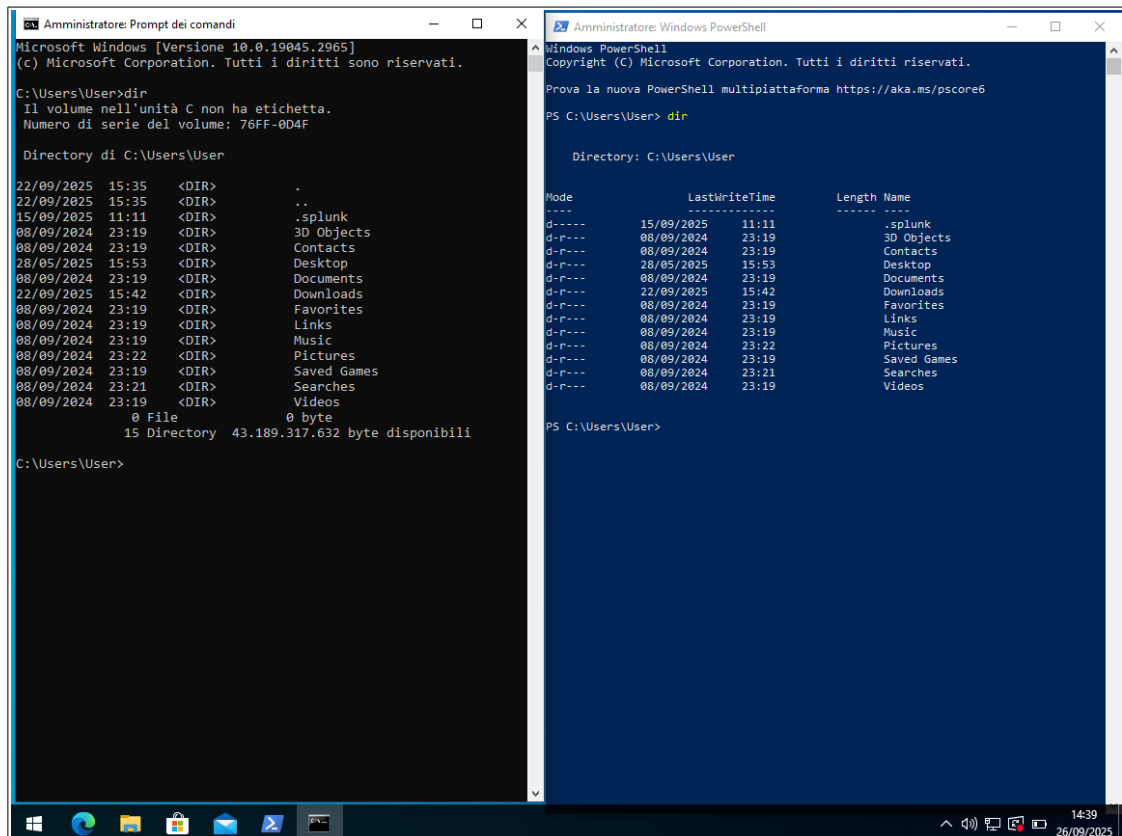
Parte 1: Accedere alla console PowerShell.

Il primo passo è stato accedere alla PowerShell e al Prompt dei Comandi per fare un confronto tra le due console.



Parte 2: Esplorare i comandi del Prompt dei Comandi e di PowerShell.

Dopodiché ho digitato lo stesso comando su entrambe le console ovvero "dir".



Quali sono gli output del comando dir?

Elenca file e sottocartelle nella directory corrente con attributi: data/ora, dimensione e nome.

Come passo successivo ho provato ad eseguire un “ping” su entrambe le console.

```
Amministratore: Prompt dei comandi
Microsoft Windows [Versione 10.0.19045.2965]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\User>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: 76FF-0D4F

Directory di C:\Users\User

22/09/2025 15:35 <DIR> .
22/09/2025 15:35 <DIR> ..
15/09/2025 11:11 <DIR> .splunk
08/09/2024 23:19 <DIR> 3D Objects
08/09/2024 23:19 <DIR> Contacts
28/05/2025 15:53 <DIR> Desktop
08/09/2024 23:19 <DIR> Documents
22/09/2025 15:42 <DIR> Downloads
08/09/2024 23:19 <DIR> Favorites
08/09/2024 23:19 <DIR> Links
08/09/2024 23:19 <DIR> Music
08/09/2024 23:22 <DIR> Pictures
08/09/2024 23:19 <DIR> Saved Games
08/09/2024 23:21 <DIR> Searches
08/09/2024 23:19 <DIR> Videos
0 File 0 byte
15 Directory 43.189.317.632 byte disponibili

C:\Users\User>ping 8.8.8.8

Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=59ms TTL=117
Risposta da 8.8.8.8: byte=32 durata=76ms TTL=117
Risposta da 8.8.8.8: byte=32 durata=55ms TTL=117
Richiesta scaduta.

Statistiche Ping per 8.8.8.8:
Pacchetti: Trasmessi = 4, Ricevuti = 3,
Persi = 1 (25% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 55ms, Massimo = 76ms, Medio = 63ms

C:\Users\User>

Amministratore: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Prova la nuova PowerShell multiplatforma https://aka.ms/pscore6

PS C:\Users\User> dir

Directory: C:\Users\User

Mode                LastWriteTime         Length Name
----                -
d-----          15/09/2025 11:11             .splunk
d-r-----        08/09/2024 23:19           3D Objects
d-r-----        08/09/2024 23:19           Contacts
d-r-----        28/05/2025 15:53           Desktop
d-r-----        08/09/2024 23:19           Documents
d-r-----        22/09/2025 15:42           Downloads
d-r-----        08/09/2024 23:19           Favorites
d-r-----        08/09/2024 23:19           Links
d-r-----        08/09/2024 23:19           Music
d-r-----        08/09/2024 23:22           Pictures
d-r-----        08/09/2024 23:19           Saved Games
d-r-----        08/09/2024 23:21           Searches
d-r-----        08/09/2024 23:19           Videos

PS C:\Users\User> ping 8.8.8.8

Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=53ms TTL=117
Risposta da 8.8.8.8: byte=32 durata=86ms TTL=117
Risposta da 8.8.8.8: byte=32 durata=117ms TTL=117
Risposta da 8.8.8.8: byte=32 durata=172ms TTL=117

Statistiche Ping per 8.8.8.8:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 53ms, Massimo = 172ms, Medio = 107ms

PS C:\Users\User>
```

Quali sono i risultati?

Entrambe le console hanno dato lo stesso risultato.

Parte 3: Esplorare i cmdlet.

Per esplorare i comandi PowerShell, chiamati cmdlet, è stato inserito il comando “Get-Alias” per elencare le sottodirectory e i file di una directory.

```
Amministratore: Windows PowerShell
PS C:\Users\User> Get-Alias dir

CommandType      Name
-----
Alias             dir -> Get-ChildItem
```

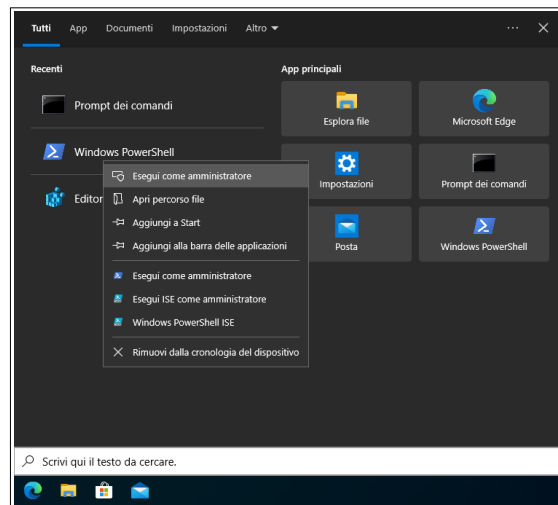
Qual è il comando PowerShell per dir?

Get-ChildItem

I cmdlet di PowerShell sono comandi nativi con sintassi verbo-nome (ad esempio Get-Process, Set-ExecutionPolicy) che operano su oggetti .NET invece che su testo, consentendo una pipeline ricca e affidabile. La documentazione ufficiale Microsoft spiega struttura, parametri, esempi e note d'uso; si possono scoprire cmdlet disponibili con Get-Command, approfondire la guida integrata con Get-Help e aprire la pagina online con Get-Help -Online, aggiornando i contenuti locali tramite Update-Help. I moduli estendono l'ambiente introducendo nuovi cmdlet specifici per ruoli e prodotti, individuabili con Get-Module e installabili da repository come PSGallery. Rispetto ai comandi tradizionali del Prompt, i cmdlet favoriscono automazione e gestione remota in modo coerente e ripetibile, risultando particolarmente utili per attività di amministrazione e sicurezza.

Parte 4: Esplorare il comando netstat usando PowerShell.

Per utilizzare alcuni comandi “netstat” (tipo “netstat -abno”) è necessario avviare PowerShell come amministratore.



1) netstat -h (elenco dei parametri disponibili e la descrizione delle opzioni)

```
Amministratore: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Prova la nuova PowerShell multiplatforma https://aka.ms/pscore6

PS C:\Users\User> netstat -h

Visualizza le statistiche del protocollo e le connessioni di rete TCP/IP correnti.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

-a Visualizza tutte le connessioni e le porte di ascolto.
-b Visualizza l'eseguibile coinvolto nella creazione di ogni connessione o
  porta di ascolto. In alcuni casi, host di eseguibili noti
  più componenti indipendenti e in questi casi il
  sequenza di componenti coinvolti nella creazione della connessione
  o la porta in ascolto. In questo caso, l'eseguibile
  il nome è in [] nella parte inferiore, in alto è il componente che ha chiamato,
  e così via fino al raggiungimento di TCP/IP. Si noti che questa opzione
  può richiedere molto tempo e avrà esito negativo, a meno che non siano sufficienti
  autorizzazioni.
-e Visualizza le statistiche Ethernet. È possibile combinare
  opzione.
-f Visualizza nomi di dominio completi (FQDN) per stranieri
  indirizzi.
-n Visualizza indirizzi e numeri di porta in formato numerico.
-o Visualizza l'ID del processo proprietario associato a ogni connessione.
-p proto Mostra le connessioni per il protocollo specificato da proto; proto
  può essere qualsiasi: TCP, UDP, TCPv6 o UDPv6. Se usato con-s
  opzione per la visualizzazione delle statistiche per protocollo, Proto può essere qualsiasi:
  IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q Visualizza tutte le connessioni, le porte di ascolto e i binding
  non in ascolto di porte TCP. Le porte di nonlistening associate possono o meno essere
  essere associate a una connessione attiva.
-r Visualizza la tabella di routing.
-s Visualizza le statistiche per protocollo. Per impostazione predefinita, le statistiche vengono
  visualizzate per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6;
  l'opzione-p può essere utilizzata per specificare un sottoinsieme del valore predefinito.
-t Visualizza lo stato corrente di offload della connessione.
-x Visualizza connessioni NetworkDirect, listener e condivisi
  endpoint.
-y Visualizza il modello di connessione TCP per tutte le connessioni.
intervallo Rivisualizza le statistiche selezionate, la sospensione dell'intervallo di secondi
  tra ogni schermo. Premere CTRL+C per interrompere la rivisualizzazione
  Statistiche. Se viene omissa, netstat stamperà il
  informazioni di configurazione una volta.

PS C:\Users\User> netstat -r

=====
Elenco interfacce
5...08 00 27 96 c2 10 .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
=====

IPv6 Tabella route
=====
```

2) netstat -r (tabella di routing del sistema)

```
Amministratore: Windows PowerShell
Non può essere combinato con le altre opzioni.
Intervallo Rivalutazione le statistiche selezionate, la sospensione dell'intervallo di secondi
tra ogni schermo. Premere CTRL+C per interrompere la rivalutazione
Statistiche. Se viene omissa, netstat stamperà il
Informazioni di configurazione una volta.

PS C:\Users\User> netstat -r

=====
Elenco Interfacce
5...00 00 27 96 c2 10 .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
=====

IPv4 Tabella route
Route attive:
Indirizzo rete      Mask      Gateway    Interfaccia Metrica
-----
0.0.0.0             0.0.0.0   192.168.50.1 127.0.0.1    25
127.0.0.0           255.0.0.0 On-link     127.0.0.1    331
127.0.0.1           255.255.255.255 On-link    127.0.0.1    331
127.255.255.255     255.255.255.255 On-link    127.0.0.1    331
192.168.50.0        255.255.255.0 On-link    192.168.50.4 281
192.168.50.4        255.255.255.255 On-link    192.168.50.4 281
224.0.0.0           240.0.0.0 On-link     127.0.0.1    331
224.0.0.0           240.0.0.0 On-link    192.168.50.4 281
255.255.255.255     255.255.255.255 On-link    127.0.0.1    331
255.255.255.255     255.255.255.255 On-link    192.168.50.4 281
=====
Route permanenti:
Nessuna

IPv6 Tabella route
Route attive:
Interf Metrica Rete Destinazione Gateway
-----
1 331 ::1/128 On-link
5 281 fe80::/64 On-link
5 281 fe80::7de5:ce64:b266:fed3/128 On-link
1 331 ff00::/8 On-link
5 281 ff00::/8 On-link
=====
Route permanenti:
Nessuna
PS C:\Users\User>
```

Qual è il gateway IPv4?

192.168.50.1

3) netstat -abno (connessioni di rete attive con informazioni molto dettagliate)

```
Amministratore: Windows PowerShell
Nessuna
PS C:\Users\User> netstat -abno

Connessioni attive
Proto Indirizzo locale      Indirizzo esterno  Stato  PID
-----
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 544
tcpip.sys
[svchost.exe]
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
Impossibile ottenere informazioni sulla proprietà
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING 1376
CDPSvc
[svchost.exe]
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING 4
Impossibile ottenere informazioni sulla proprietà
TCP 0.0.0.0:7680 0.0.0.0:0 LISTENING 4560
Impossibile ottenere informazioni sulla proprietà
TCP 0.0.0.0:8080 0.0.0.0:0 LISTENING 2764
[splunkd.exe]
TCP 0.0.0.0:8089 0.0.0.0:0 LISTENING 2764
[splunkd.exe]
TCP 0.0.0.0:8191 0.0.0.0:0 LISTENING 5696
[mongod.exe]
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 836
[lsass.exe]
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING 672
Impossibile ottenere informazioni sulla proprietà
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING 1224
Eventlog
[svchost.exe]
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING 1088
Schedule
[svchost.exe]
TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING 2348
[spoolsv.exe]
TCP 0.0.0.0:49673 0.0.0.0:0 LISTENING 812
Impossibile ottenere informazioni sulla proprietà
TCP 127.0.0.1:8065 0.0.0.0:0 LISTENING 7732
[Python3.9.exe]
TCP 127.0.0.1:8089 127.0.0.1:49773 ESTABLISHED 2764
[splunkd.exe]
TCP 127.0.0.1:8089 127.0.0.1:49864 ESTABLISHED 2764
[splunkd.exe]
TCP 127.0.0.1:8089 127.0.0.1:50207 ESTABLISHED 2764
[splunkd.exe]
TCP 127.0.0.1:8191 127.0.0.1:49777 ESTABLISHED 5696
[mongod.exe]
TCP 127.0.0.1:8191 127.0.0.1:49780 ESTABLISHED 5696
[mongod.exe]
TCP 127.0.0.1:8191 127.0.0.1:49781 ESTABLISHED 5696
[mongod.exe]
TCP 127.0.0.1:8191 127.0.0.1:49782 ESTABLISHED 5696
[mongod.exe]
TCP 127.0.0.1:8191 127.0.0.1:49790 ESTABLISHED 5696
[mongod.exe]
TCP 127.0.0.1:8191 127.0.0.1:49791 ESTABLISHED 5696
```

Nell'output di netstat -abno sono presenti dei PID ovvero dei numeri univoci che il sistema operativo assegna a ogni processo in esecuzione. Le proprietà dei PID possono essere analizzati dal Task Manager.

The screenshot shows a Windows PowerShell window with the command `netstat -abno` executed. The output lists active connections with columns for Protocol, Local Address, Remote Address, State, and PID. A context menu is open over the Task Manager window, showing options like 'Termina attività', 'Termina albero processi', 'Invia feedback', 'Imposta priorità', 'Imposta affinità', 'Analizza catena di attesa', 'Virtualizzazione controllo dell'account utente', 'Crea file di dettagli', 'Apri percorso file', 'Cerca online', 'Proprietà', and 'Vai ai servizi'. The 'Proprietà' option is selected.

Proto	Indirizzo locale	Indirizzo esterno	Stato	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	544
RpcEptMapper				
[svchost.exe]				
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	1376
CDPSvc				
[svchost.exe]				
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING	4560
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:8000	0.0.0.0:0	LISTENING	2764
[splunkd.exe]				
TCP	0.0.0.0:8089	0.0.0.0:0	LISTENING	2764
[splunkd.exe]				
TCP	0.0.0.0:8191	0.0.0.0:0	LISTENING	5696
[mongod.exe]				
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	836
[lsass.exe]				
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	672
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1224
EventLog				
[svchost.exe]				
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	1088
Schedule				
[svchost.exe]				
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	2348
[spoolsv.exe]				
TCP	0.0.0.0:49673	0.0.0.0:0	LISTENING	812
Impossibile ottenere informazioni sulla proprietà				
TCP	127.0.0.1:8065	0.0.0.0:0	LISTENING	7732
[Python3.9.exe]				
TCP	127.0.0.1:8089	127.0.0.1:49773	ESTABLISHED	2764
[splunkd.exe]				
TCP	127.0.0.1:8089	127.0.0.1:49864	ESTABLISHED	2764
[splunkd.exe]				
TCP	127.0.0.1:8089	127.0.0.1:50207	ESTABLISHED	2764
[splunkd.exe]				
TCP	127.0.0.1:8191	127.0.0.1:49777	ESTABLISHED	5696
[mongod.exe]				
TCP	127.0.0.1:8191	127.0.0.1:49780	ESTABLISHED	5696
[mongod.exe]				
TCP	127.0.0.1:8191	127.0.0.1:49781	ESTABLISHED	5696
[mongod.exe]				
TCP	127.0.0.1:8191	127.0.0.1:49782	ESTABLISHED	5696
[mongod.exe]				
TCP	127.0.0.1:8191	127.0.0.1:49790	ESTABLISHED	5696
[mongod.exe]				
TCP	127.0.0.1:8191	127.0.0.1:49791	ESTABLISHED	5696
[mongod.exe]				

The screenshot shows a Windows PowerShell window with the command `netstat -abno` executed. The output lists active connections with columns for Protocol, Local Address, Remote Address, State, and PID. A context menu is open over the Task Manager window, showing options like 'Termina attività', 'Termina albero processi', 'Invia feedback', 'Imposta priorità', 'Imposta affinità', 'Analizza catena di attesa', 'Virtualizzazione controllo dell'account utente', 'Crea file di dettagli', 'Apri percorso file', 'Cerca online', 'Proprietà', and 'Vai ai servizi'. The 'Proprietà' option is selected.

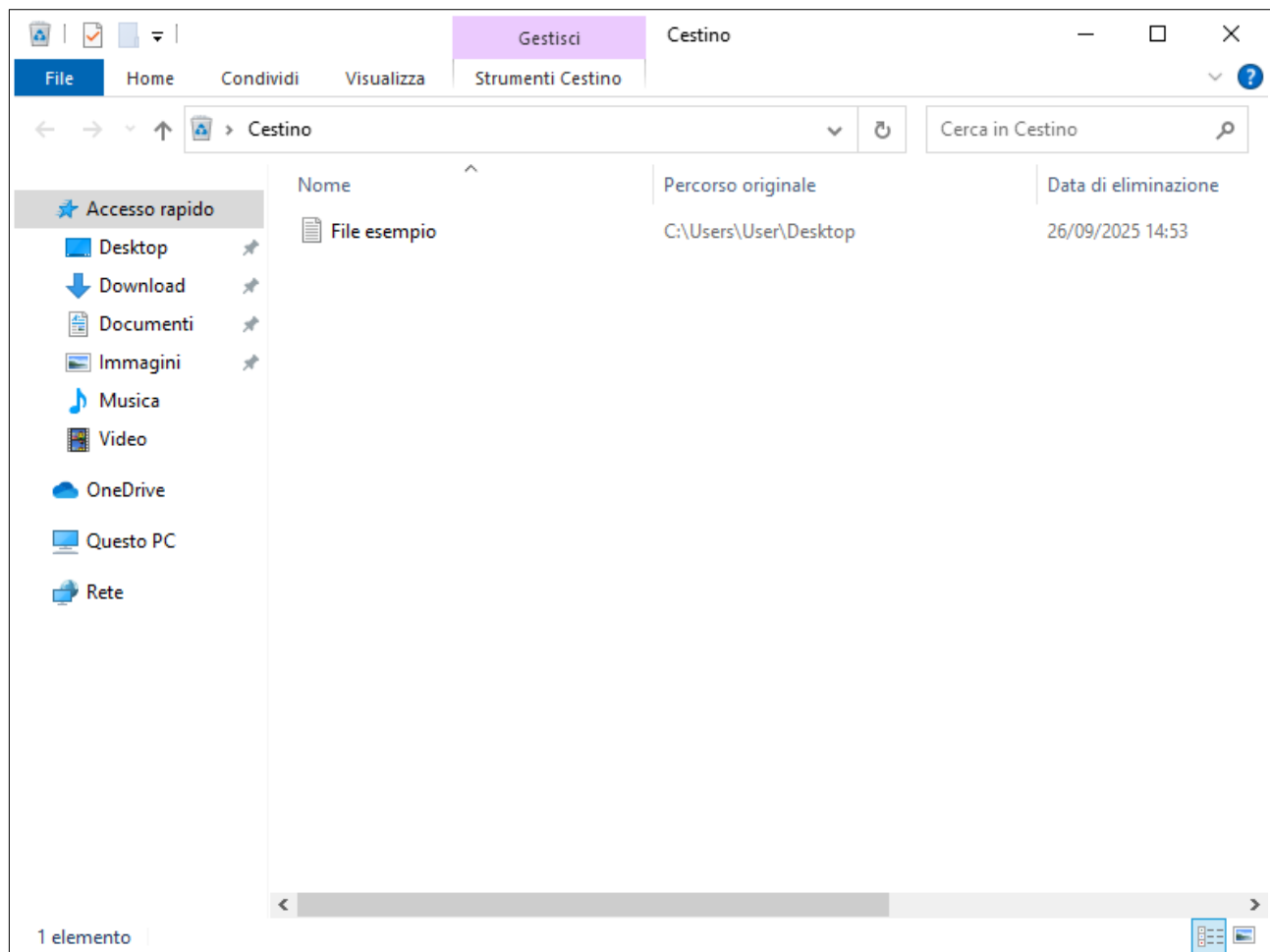
Proto	Indirizzo locale	Indirizzo esterno	Stato	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	544
RpcEptMapper				
[svchost.exe]				
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	1376
CDPSvc				
[svchost.exe]				
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING	4560
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:8000	0.0.0.0:0	LISTENING	2764
[splunkd.exe]				
TCP	0.0.0.0:8089	0.0.0.0:0	LISTENING	2764
[splunkd.exe]				
TCP	0.0.0.0:8191	0.0.0.0:0	LISTENING	5696
[mongod.exe]				
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	836
[lsass.exe]				
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	672
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1224
EventLog				
[svchost.exe]				
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	1088
Schedule				
[svchost.exe]				
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	2348
[spoolsv.exe]				
TCP	0.0.0.0:49673	0.0.0.0:0	LISTENING	812
Impossibile ottenere informazioni sulla proprietà				
TCP	127.0.0.1:8065	0.0.0.0:0	LISTENING	7732
[Python3.9.exe]				
TCP	127.0.0.1:8089	127.0.0.1:49773	ESTABLISHED	2764
[splunkd.exe]				
TCP	127.0.0.1:8089	127.0.0.1:49864	ESTABLISHED	2764
[splunkd.exe]				
TCP	127.0.0.1:8089	127.0.0.1:50207	ESTABLISHED	2764
[splunkd.exe]				
TCP	127.0.0.1:8191	127.0.0.1:49777	ESTABLISHED	5696
[mongod.exe]				
TCP	127.0.0.1:8191	127.0.0.1:49780	ESTABLISHED	5696
[mongod.exe]				
TCP	127.0.0.1:8191	127.0.0.1:49781	ESTABLISHED	5696
[mongod.exe]				
TCP	127.0.0.1:8191	127.0.0.1:49782	ESTABLISHED	5696
[mongod.exe]				
TCP	127.0.0.1:8191	127.0.0.1:49790	ESTABLISHED	5696
[mongod.exe]				
TCP	127.0.0.1:8191	127.0.0.1:49791	ESTABLISHED	5696
[mongod.exe]				

Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?

Nome dell'eseguibile, percorso file, dimensione, versione, firma digitale (se presente), utente che esegue il processo, data di creazione, uso CPU/memoria corrente.

Parte 5: Svuotare il cestino usando PowerShell.

Da PowerShell si possono eseguire anche comandi di gestione del computer. Come esempio è stato usato il comando "Clear-RecycleBin" per svuotare il cestino.

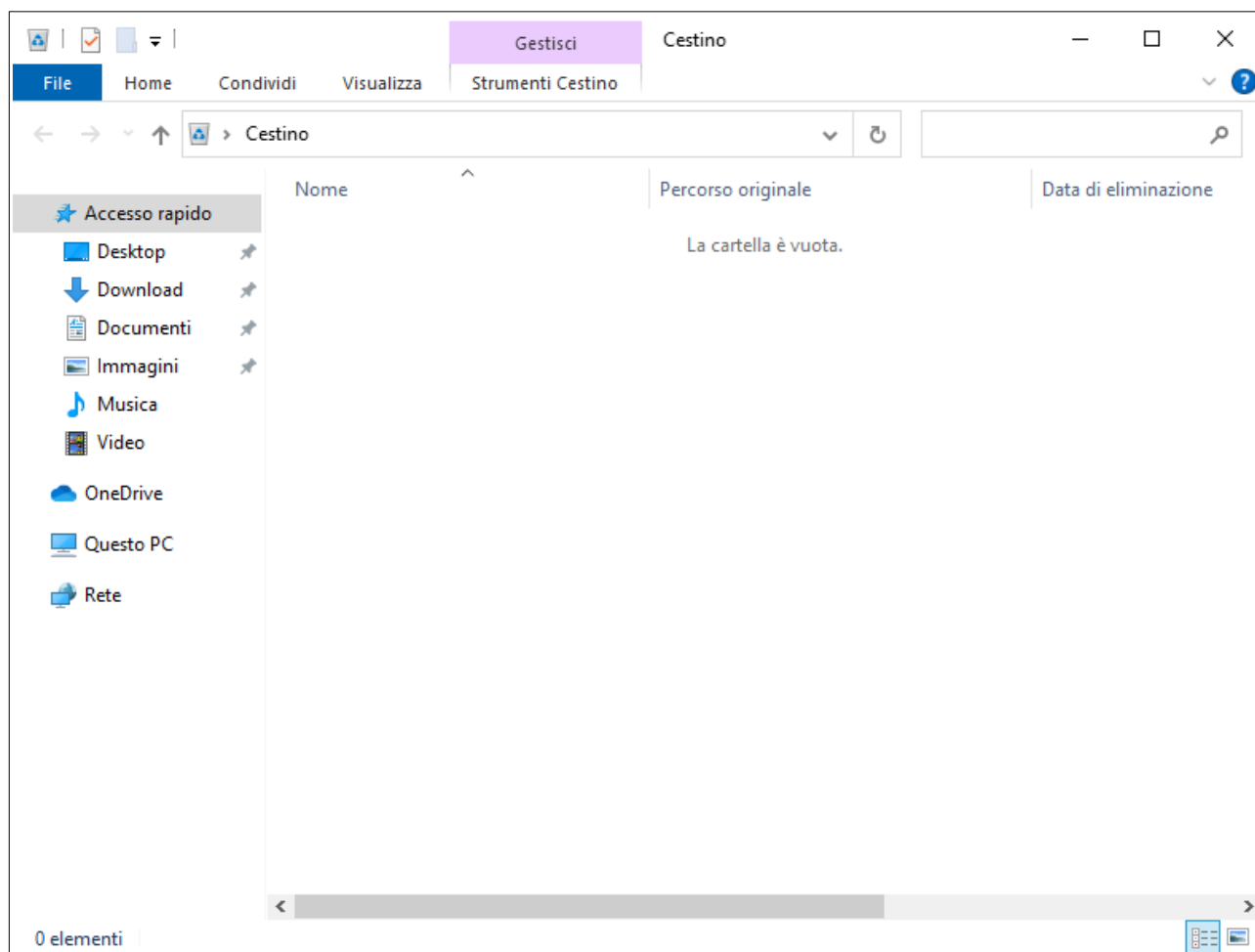


```
Amministratore: Windows PowerShell
PS C:\Users\User> Clear-RecycleBin

Conferma
Eeguire l'operazione?
Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino".
[S] Sì [T] Sì a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida (il valore predefinito è "S"): s
PS C:\Users\User>
```

Cosa è successo ai file nel Cestino?

Il file di testo all'interno del cestino è stato eliminato definitivamente.



Conclusione

PowerShell rappresenta uno strumento molto potente per semplificare e automatizzare le attività quotidiane legate alla sicurezza e all'amministrazione di un sistema. Grazie ai cmdlet è possibile interrogare in tempo reale processi, servizi, log di sistema e connessioni di rete senza dover ricorrere a strumenti grafici o a utility esterne, con il vantaggio di poter integrare tutto in script riutilizzabili. Per un analista di sicurezza, comandi come Get-Process e Get-Service permettono di monitorare in modo immediato lo stato delle applicazioni, Get-EventLog consente di analizzare gli eventi registrati dal sistema, mentre Get-NetTCPConnection e Test-NetConnection forniscono informazioni utili sulle connessioni di rete e la raggiungibilità di host remoti. Anche Get-ChildItem -Recurse risulta utile per esplorare file e directory alla ricerca di contenuti sospetti. L'uso combinato di questi strumenti consente di aumentare il livello di controllo, velocizzare indagini e verifiche e ridurre i margini di errore umano.

Studio Ioc

Introduzione

Obiettivo dell'esercizio: analizzare il report AnyRun relativo un campione potenzialmente malevolo e produrre una sintesi tecnica che descriva il comportamento osservato, le tattiche/tecniche utilizzate e gli indicatori di compromissione (IoC).

Profilo del campione (Jvczfhe.exe)

Verdetto di AnyRun: Malicious Activity

Hash segnalato da AnyRun:

MD5: 00B5E91B42712471CDFBDB37B715670C

SHA1: D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2

SHA256: 0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0

Sintesi delle tattiche e tecniche osservate

Esecuzione

- Drop e uso di file .exe secondari (Muadnrd.exe), esecuzioni tramite processi legittimi (InstallUtil.exe) e iterazioni con WerFault.exe (Windows Error Reporting).
- Abuso di LOLBins: InstallUtil.exe e processi legittimi per eseguire o mascherare codice malevolo.

Evasione e anti-analisi

- Uso di timeout.exe per introdurre ritardi (tecnica anti-sandbox).
- Induzione di crash e gestione tramite WerFault, probabilmente per deviare log/artefatti o alterare il flusso di esecuzione.

Fingerprinting e raccolta dati

- Lettura di informazioni di sistema: nome macchina, Machine GUID, variabili d'ambiente, lingue supportate.
- Lettura chiavi relative a Microsoft Office e impostazioni Internet Explorer / WinINET.

Anti-forensics / Anti-logging

- Modifiche al registro per disattivare il RAS tracing relative ai nomi dei processi coinvolti:
 - HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_*
 - HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_*Valori impostati su EnableFileTracing=0, EnableAutoFileTracing=0, EnableConsoleTracing=0, ecc per ridurre i log e maggiore difficoltà nelle attività di analisi forense.

Manipolazione delle impostazioni di rete (WinINET/IE)

- Scritture in HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
 - ProxyBypass=1, IntranetName=1, UNCAsIntranet=1, AutoDetect=0.Effetto: bypass proxy e considerazione di risorse UNC come Intranet (zone più permissive), agevolando comunicazioni esterne e aggirando controlli di rete.

Artefatti di crash e identità

- WerFault genera dump (*.dmp) e report WER per Jvczfhe.exe e Muadnrd.exe.
- Sono presenti scritture sensibili in HKCU\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\... (DeviceTicket, AppInit_DLLs) possibili artefatti collegati a identità o token utente.

Persistenza

Nel blocco analizzato non sono state rilevate scritture classiche per persistenza. Possibile spiegazione:

- persistenza implementata in fasi successive non osservate.
- tentativi falliti a causa di crash.
- modalità fileless o persistente tramite meccanismi non tipici. Va verificato con analisi Process tree / Autoruns / EDR.

Valutazione funzionale

Il comportamento è coerente con un trojan loader/dropper offuscato (.NET) che:

- esegue fingerprinting e raccolta ambiente.
- disabilita/trama log per nascondere attività.
- Modifica impostazioni di rete per facilitare comunicazioni.
- scarica/avvia payload secondari (Muadnrd.exe).
- sfrutta strumenti legittimi per esecuzione e mascheramento.

Conclusione: si classifica come un Trojan Loader/Dropper (con possibili funzionalità di infostealer) piuttosto che ransomware o worm.

Indicatori di Compromissione (IoC) consolidati

Hash (dal dump)

- Jvczfhe.exe (Downloads): SHA256
E6A7AAFF54EB6D06ACFC6F1DFA21A85B767DBF7FF3E9BFDF2DDBDECED86AA9B2
- Muadnrd.exe (Downloads): SHA256
B662E7213F4985684439E655BD92EA4B9A1566E76712BB86E1238113A35B90A0

Percorsi e artefatti

- C:\Users\admin\Downloads\Jvczfhe.exe (+ :Zone.Identifier)
- C:\Users\admin\Downloads\Muadnrd.exe (+ :ZoneIdentifier)
- Crash dumps e report:
 - C:\Users\admin\AppData\Local\CrashDumps*.dmp
 - C:\ProgramData\Microsoft\Windows\WER\ReportArchive\...\Report.wer
 - C:\ProgramData\Microsoft\Windows\WER\Temp*.dmp, *.xml

Chiavi di registro modificate

- Anti-logging RAS:
 - HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32|RASMANCS
 - HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32|RASMANCS
(DeviceTicket / DeviceId / ApplicationFlags)

Conclusione

L'analisi mostra un campione offuscato (.NET Reactor) che si comporta come trojan loader/dropper, con chiare misure di evasione e anti-forensics, e con capacità di preparare la rete e il sistema per successive comunicazioni o download di payload. Sebbene non siano emerse evidenze di cifratura tipiche di ransomware, il comportamento è pericoloso: raccomandata immediata azione di containment, raccolta prove e bonifica seguendo le raccomandazioni fornite.