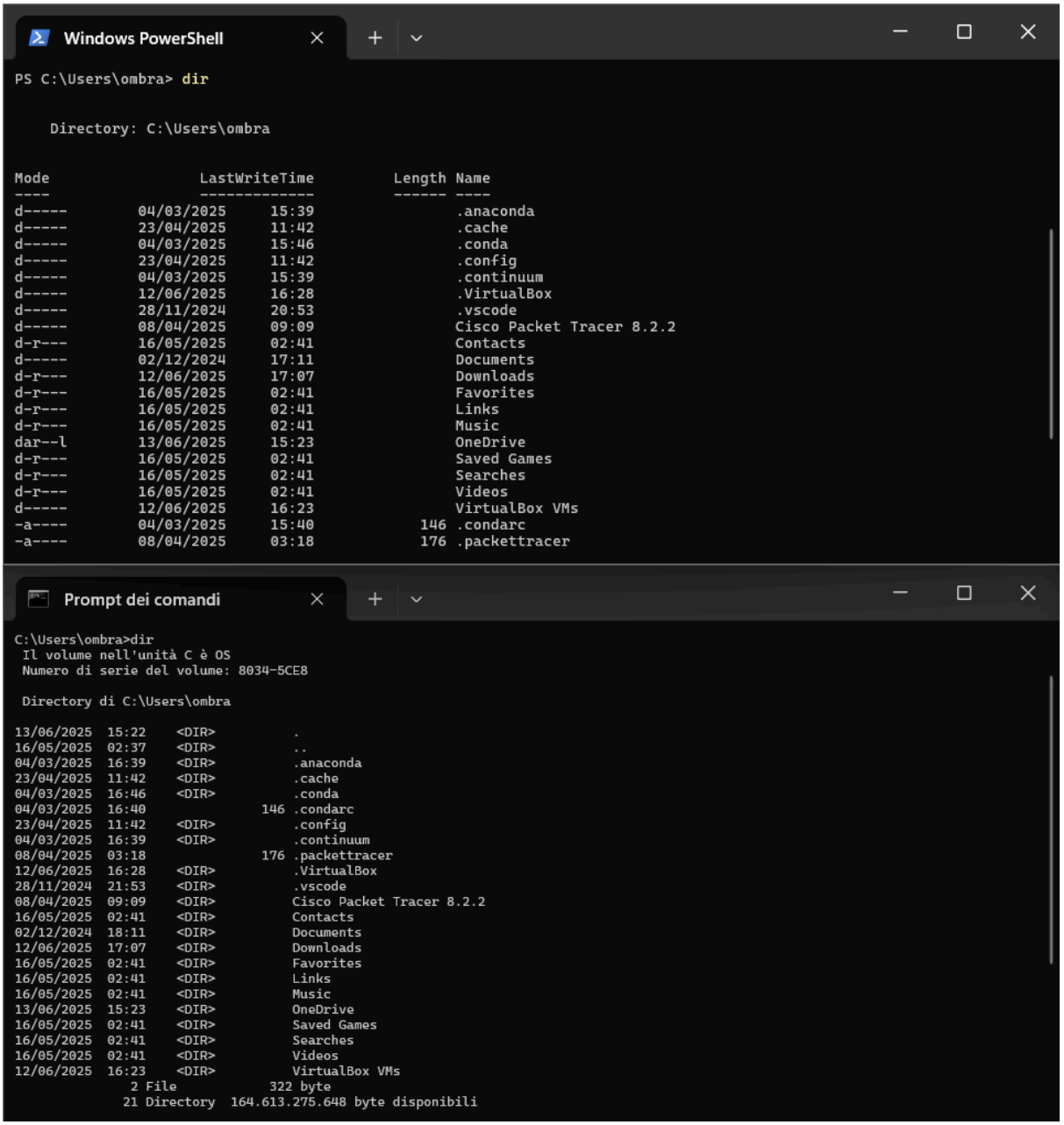
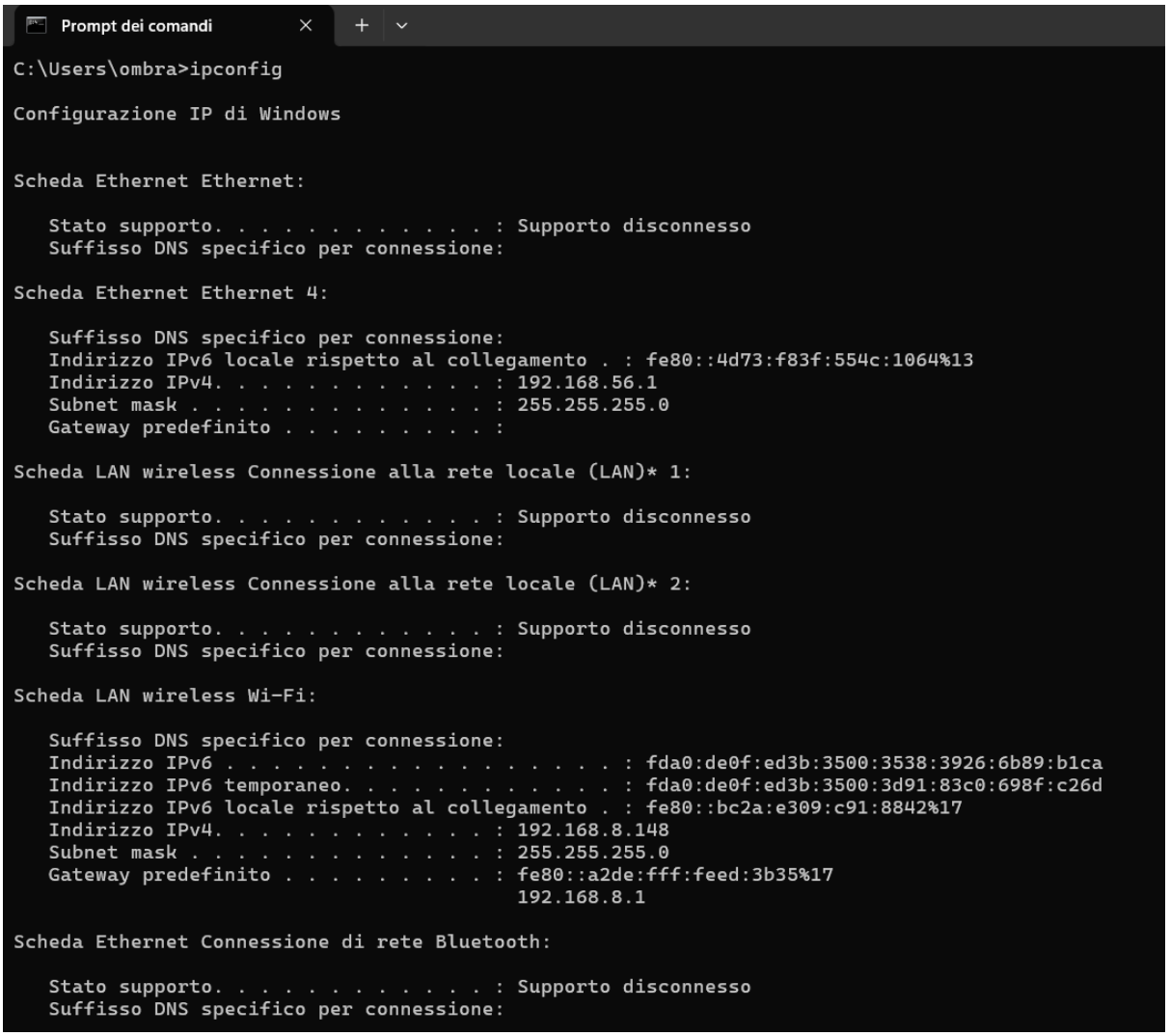
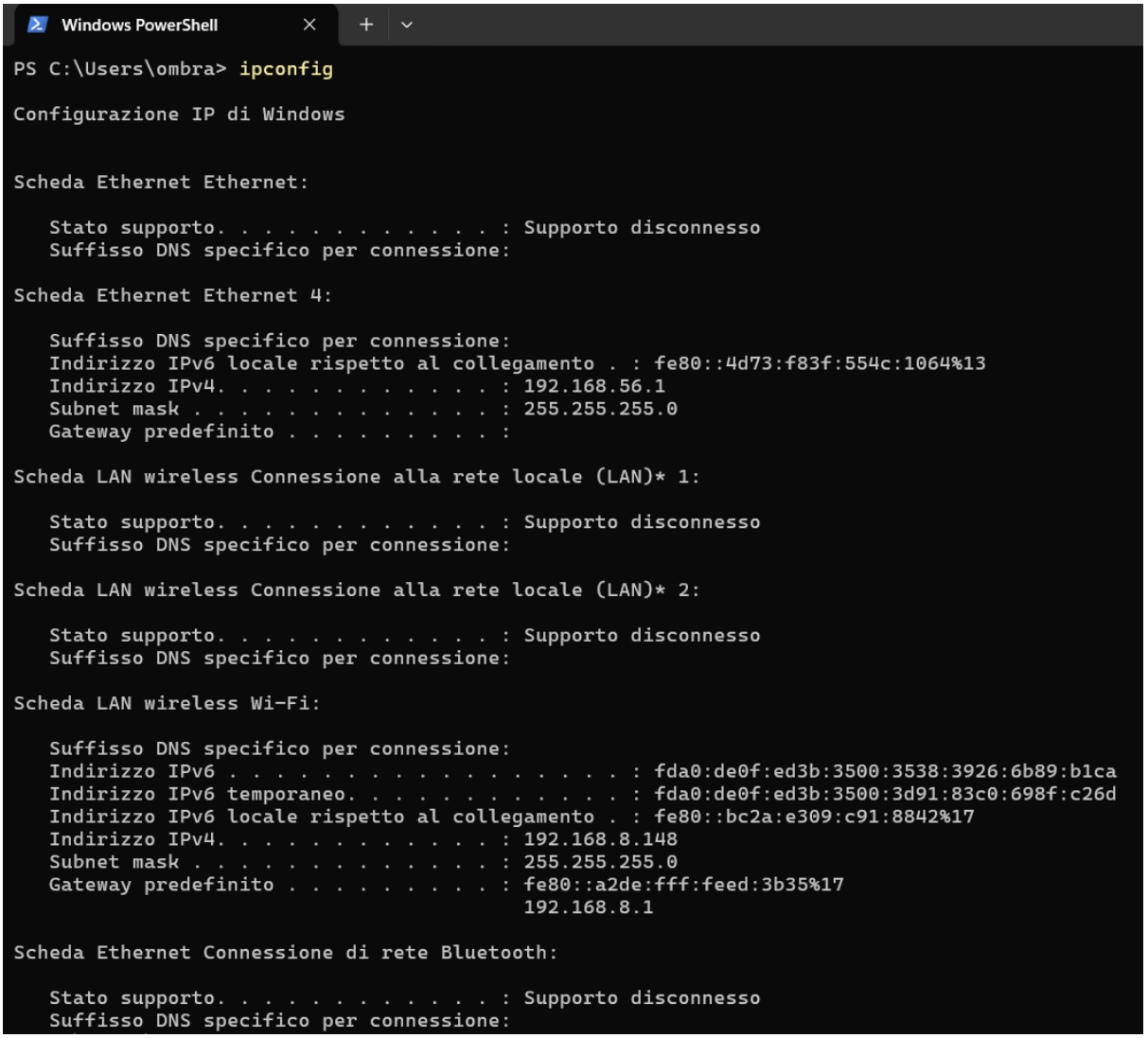
Progetto 13/06

Quali sono gli output del comando dir?



Quali sono i risultati di ipconfig?





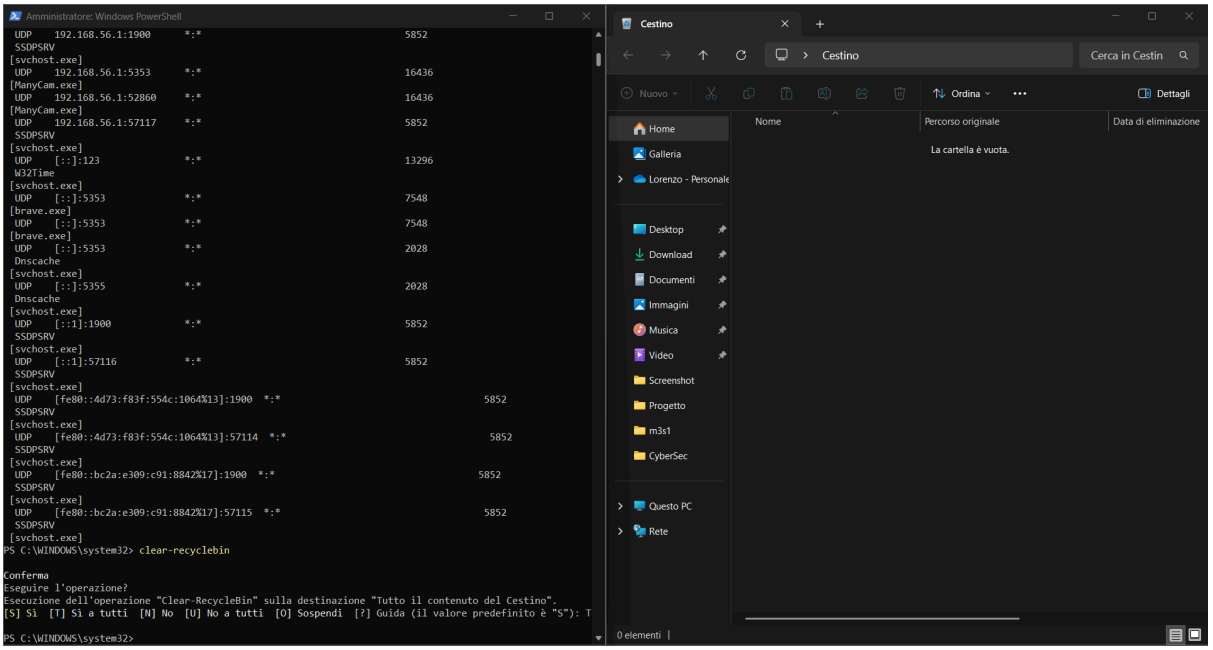
Qual è il comando PowerShell per dir?

Get-Children

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

Proprietà	Valore
Descrizione	
Descrizione del file	Processo host per servizi di Windows
Tipo	Applicazione
Versione file	10.0.26100.4343
Nome prodotto	Sistema operativo Microsoft® Windows®
Versione	10.0.26100.4343
Copyright	© Microsoft Corporation. Tutti i diritti riservati.
Dimensione	86,2 KB
Ultima modifica	10/06/2025 22:34
Lingua	Italiano (Italia)
Nome file originale	svchost.exe

Cosa è successo ai file nel Cestino?



Report Analisi Malware – Esercizio 2

Link analisi:
https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/

Descrizione generale

Il file esaminato presenta comportamenti sospetti, come l'autolancio, l'esecuzione di comandi da terminale e l'accesso a chiavi di registro legate alla sicurezza. Inoltre, l'applicazione va in crash, potenzialmente come tecnica di evasione.

Comportamento osservato

- Esegue un'applicazione che **crasha**.
- Il processo **si auto-lancia**.
- Accesso a chiavi di registro relative a:
    - **Impostazioni di sicurezza di Internet Explorer**
    - **Trust Settings di Windows**
- Avvio della **shell di comando (cmd.exe)**.

Tecniche MITRE ATT&CK rilevate

- **T1012 – Query Registry**
  Lettura di chiavi di registro per raccogliere informazioni su impostazioni di sicurezza.
- **T1059.003 – Command and Scripting Interpreter: Windows Command Shell**
  Esecuzione di **cmd.exe** per impartire comandi al sistema.

Conclusioni

Il comportamento osservato è coerente con una minaccia mirata a:

- Raccogliere informazioni sul sistema.
- Eseguire comandi in locale.
- Bypassare meccanismi di sicurezza.

Il comportamento rilevato suggerisce la presenza di un malware di tipo dropper/infostealer con capacità di comunicazione via DNS verso ***.duckdns.org**.

Consigli:

1. Bloccare i domini **duckdns.org** a livello firewall/DNS.
2. Monitorare e isolare le richieste di **cmd.exe** e i crash inattesi.
3. Aggiornare le regole di rilevamento per query DNS dinamiche.