

Progetto 13/06

Quali sono gli output del comando dir?

```
Windows PowerShell
PS C:\Users\ombra> dir

Directory: C:\Users\ombra

Mode                LastWriteTime         Length Name
----                -
d-----          04/03/2025         15:39      .anaconda
d-----          23/04/2025         11:42      .cache
d-----          04/03/2025         15:46      .conda
d-----          23/04/2025         11:42      .config
d-----          04/03/2025         15:39      .continuum
d-----          12/06/2025         16:28      .VirtualBox
d-----          28/11/2024         20:53      .vscode
d-----          08/04/2025          09:09      Cisco Packet Tracer 8.2.2
d-r-----        16/05/2025          02:41      Contacts
d-----          02/12/2024         17:11      Documents
d-r-----        12/06/2025         17:07      Downloads
d-r-----        16/05/2025          02:41      Favorites
d-r-----        16/05/2025          02:41      Links
d-r-----        16/05/2025          02:41      Music
dar--l          13/06/2025         15:23      OneDrive
d-r-----        16/05/2025          02:41      Saved Games
d-r-----        16/05/2025          02:41      Searches
d-r-----        16/05/2025          02:41      Videos
d-----          12/06/2025         16:23      VirtualBox VMs
-a-----          04/03/2025         15:40      146 .condarc
-a-----          08/04/2025          03:18      176 .packettracer

Prompt dei comandi
C:\Users\ombra>dir
Il volume nell'unità C è OS
Numero di serie del volume: 8034-5CE8

Directory di C:\Users\ombra

13/06/2025  15:22  <DIR>      .
16/05/2025  02:37  <DIR>      ..
04/03/2025  16:39  <DIR>      .anaconda
23/04/2025  11:42  <DIR>      .cache
04/03/2025  16:46  <DIR>      .conda
04/03/2025  16:40      146 .condarc
23/04/2025  11:42  <DIR>      .config
04/03/2025  16:39  <DIR>      .continuum
08/04/2025  03:18      176 .packettracer
12/06/2025  16:28  <DIR>      .VirtualBox
28/11/2024  21:53  <DIR>      .vscode
08/04/2025  09:09  <DIR>      Cisco Packet Tracer 8.2.2
16/05/2025  02:41  <DIR>      Contacts
02/12/2024  18:11  <DIR>      Documents
12/06/2025  17:07  <DIR>      Downloads
16/05/2025  02:41  <DIR>      Favorites
16/05/2025  02:41  <DIR>      Links
16/05/2025  02:41  <DIR>      Music
13/06/2025  15:23  <DIR>      OneDrive
16/05/2025  02:41  <DIR>      Saved Games
16/05/2025  02:41  <DIR>      Searches
16/05/2025  02:41  <DIR>      Videos
12/06/2025  16:23  <DIR>      VirtualBox VMs
      2 File          322 byte
      21 Directory 164.613.275.648 byte disponibili
```

Quali sono i risultati di ipconfig?

```
Prompt dei comandi
C:\Users\ombra>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda Ethernet Ethernet 4:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::4d73:f83f:554c:1064%13
    Indirizzo IPv4. . . . . : 192.168.56.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda LAN wireless Connessione alla rete locale (LAN)* 1:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda LAN wireless Connessione alla rete locale (LAN)* 2:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda LAN wireless Wi-Fi:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : fda0:de0f:ed3b:3500:3538:3926:6b89:b1ca
    Indirizzo IPv6 temporaneo. . . . . : fda0:de0f:ed3b:3500:3d91:83c0:698f:c26d
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::bc2a:e309:c91:8842%17
    Indirizzo IPv4. . . . . : 192.168.8.148
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : fe80::a2de:fff:feed:3b35%17
                                     192.168.8.1

Scheda Ethernet Connessione di rete Bluetooth:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:
```

```
Windows PowerShell
PS C:\Users\ombra> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda Ethernet Ethernet 4:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::4d73:f83f:554c:1064%13
    Indirizzo IPv4. . . . . : 192.168.56.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda LAN wireless Connessione alla rete locale (LAN)* 1:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda LAN wireless Connessione alla rete locale (LAN)* 2:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda LAN wireless Wi-Fi:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : fda0:de0f:ed3b:3500:3538:3926:6b89:b1ca
    Indirizzo IPv6 temporaneo. . . . . : fda0:de0f:ed3b:3500:3d91:83c0:698f:c26d
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::bc2a:e309:c91:8842%17
    Indirizzo IPv4. . . . . : 192.168.8.148
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : fe80::a2de:fff:feed:3b35%17
                                   192.168.8.1

Scheda Ethernet Connessione di rete Bluetooth:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:
```

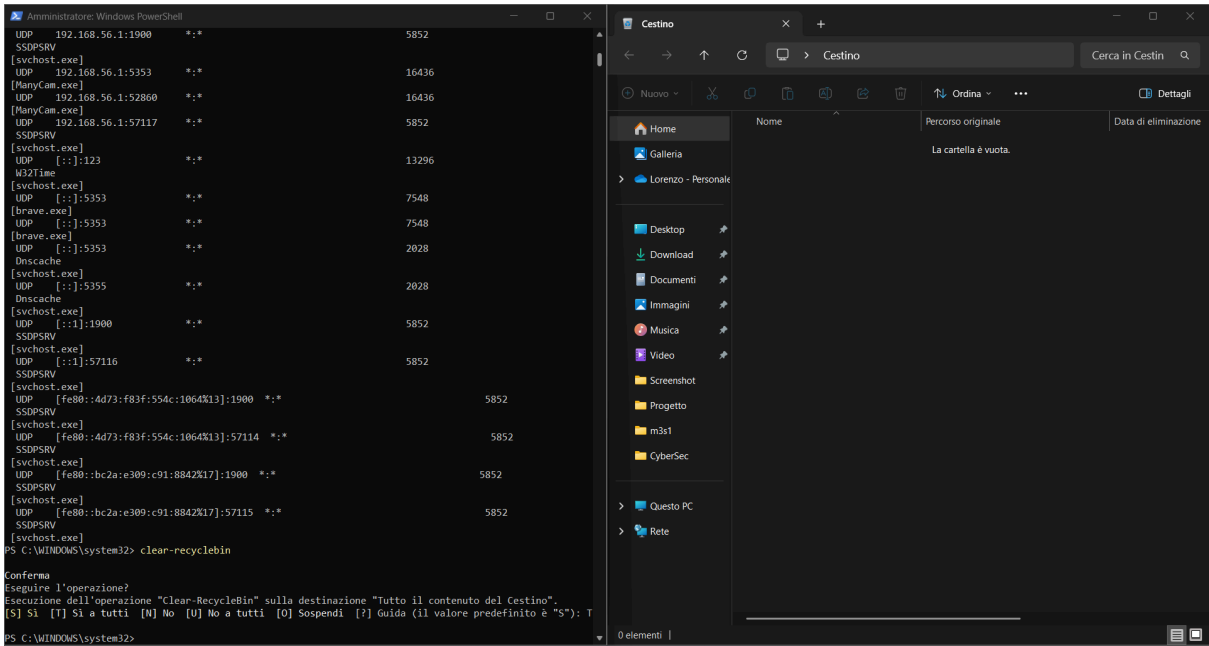
Qual è il comando PowerShell per dir?

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.