## Report di Analisi sugli Attacchi

### 1. Task 1

**URL:** https://app.any.run/tasks/685ba854-4644-4140-9ea5-be9057161248/

**Descrizione:** L'analisi del task indica un attacco basato su un file eseguibile sospetto. Durante l'esecuzione, il malware tenta di connettersi a vari indirizzi IP remoti e scaricare ulteriori componenti dannosi. Sono stati rilevati tentativi di alterazione del registro di sistema e apertura di connessioni di rete non autorizzate.

**Conclusioni:**

- Possibile infezione da malware con capacità di connessione remota.
- Alterazioni del sistema che potrebbero compromettere la sicurezza.

### 2. Task 2

**URL:** https://app.any.run/tasks/8a2c185d-5a11-4aac-9286-43c641e1991a/

**Descrizione:** L'analisi mostra un attacco tramite script PowerShell che tenta di modificare le impostazioni DNS del sistema. Lo script cerca di cambiare i server DNS a favore di quelli controllati dall'attaccante, potenzialmente per reindirizzare il traffico internet degli utenti verso siti malevoli.

**Conclusioni:**

- Attacco mirato a modificare le impostazioni DNS.
- Rischio di dirottamento del traffico internet e possibile phishing.

## Raccomandazioni

- **Isolare immediatamente i sistemi compromessi.**
- **Eseguire una scansione completa del sistema alla ricerca di ulteriori minacce.**
- **Ripristinare le impostazioni DNS e di registro di sistema.**
- **Monitorare il traffico di rete per attività sospette.**
- **Aggiornare tutte le credenziali di accesso e implementare ulteriori misure di sicurezza.**