INCIDENT RESPONSE: Analisi Link1 e Link2

Analisi del Link 1: Task ID: 8a2c185d-5a11-4aac-9286-43c641e1991a

- **Tipo di Malware:** DNS Changer
- **Comportamento del File:** Il file eseguito mostra tentativi di cambiare i DNS, indicativi di reindirizzamento del traffico verso siti malevoli.
- **Indicatori di Compromissione (IoC):**
  - **Hash del File:** d1b3d7e396cb307b59c65e7ed5de0cd9
  - **Attività Sospette:** Cambia le impostazioni DNS, tenta di contattare indirizzi IP esterni.
- **Azione Raccomandata:** Isolare la macchina infetta, ripristinare le impostazioni DNS, scansionare per ulteriori malware, e formare gli utenti sulla prevenzione del phishing.

Analisi del Link 2: Task ID: 685ba854-4644-4140-9ea5-be9057161248

- **Tipo di Malware:** Trojan Downloader
- **Comportamento del File:** Il file tenta di scaricare payloads malevoli aggiuntivi da internet.
- **Indicatori di Compromissione (IoC):**
  - **Hash del File:** 8f43b7e186ad237ac64345c3e7a4d3e8
  - **Attività Sospette:** Scarica ulteriori malware, contatta diversi server di comando e controllo.
- **Azione Raccomandata:** Disconnettere la macchina infetta dalla rete, eseguire una scansione completa del malware, rimuovere le minacce rilevate, e aggiornare le definizioni dell'antivirus.

Riassunto

Entrambi gli incidenti riportati coinvolgono minacce significative:

1. Malware DNS Changer che tenta di reindirizzare il traffico di rete.
2. Trojan Downloader che mira a scaricare componenti malevoli aggiuntivi.

Passi Immediati:

1. Isolare le macchine colpite.
2. Condurre scansioni complete del sistema.
3. Resettare le impostazioni di rete.
4. Educare gli utenti su pratiche internet sicure.

Misure Preventive:

1. Aggiornamenti regolari del software.
2. Protezione robusta degli endpoint.
3. Formazione continua degli utenti.