Consegna S9-L2

Consegna: Attività di Analisi del Malware AgentTesla

⚜️ **Tag:** #agenttesla #malware #cuckoo #virustotal #analisi

Oggetto

Sarà condiviso un malware relativamente innocuo: **AgentTesla**.

Compiti

1. **Analisi Statica:**
   - Esaminare il codice del malware senza eseguirlo, al fine di comprendere la sua struttura e le sue funzionalità.
   - Strumenti utilizzati:
     - **VirusTotal**: Per identificare firme e rilevamenti preesistenti del malware.
     - **Hex Editor**: Per ispezionare il codice binario.
     - **Strings**: Per estrarre stringhe leggibili dal file binario.
2. **Analisi Dinamica:**
   - Eseguire il malware in un ambiente controllato per osservare il suo comportamento e identificare le sue azioni in tempo reale.
   - Strumenti utilizzati:
     - **Cuckoo Sandbox**: Per analizzare il comportamento del malware in un ambiente isolato.
     - **Wireshark**: Per monitorare eventuali connessioni di rete generate dal malware.
     - **Procmon**: Per tracciare le azioni del malware nel sistema operativo (es. creazione di file, modifica del registro).

Output Attesi

1. **Report Statica:**
    - Rilevamenti VirusTotal con hash del file.
    - Stringhe sospette estratte dal file.
    - Annotazioni sul formato e le funzionalità identificate nel codice binario.
2. **Report Dinamica:**
    - Log delle connessioni di rete catturate con Wireshark.
    - Azioni del malware registrate da Procmon.
    - Screenshot e report generati dalla Cuckoo Sandbox.

Conclusione

Questa attività permette di comprendere come un malware come AgentTesla opera sia in termini statici che dinamici. Gli strumenti utilizzati evidenziano la sua pericolosità e le tecniche per mitigarne l'impatto nel contesto della cybersecurity.

🔑 **Chiavi:**
[agenttesla, malware, cuckoo, virustotal, analisi]