# Relazione sull'analisi del malware "AgentTesla.exe"

## 1. Analisi Statica

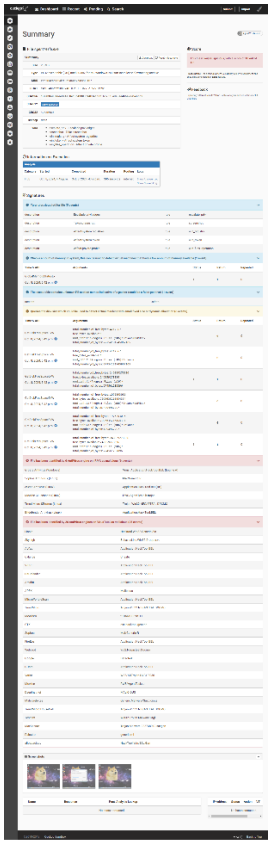
L'analisi statica permette di valutare il malware "AgentTesla.exe" senza eseguirlo, analizzandone la struttura interna e il codice.

- **Tipo di file**: "AgentTesla.exe" è un eseguibile PE32 (Portable Executable) di tipo GUI (Graphical User Interface), progettato per architetture Intel 80386 a 32 bit e Windows. La dimensione del file è di circa 2.8MB, e il file è un archivio autoestraente creato con **Nullsoft Installer**, che potrebbe essere un indizio del tentativo di camuffare il malware sotto forma di installer legittimo.
- **Hash**: Le firme hash (MD5, SHA1, SHA256, SHA512) confermano che questo file è noto e già segnalato su piattaforme di sicurezza. La firma MD5 corrisponde a quella di malware rilevati, come indicato nella sezione seguente sull'analisi dinamica.
- **Indicatori Yara**: Le regole Yara applicate al file mostrano indicazioni di funzionalità dannose:
    - **escalate_priv**: Implica che il malware tenti di eseguire operazioni per elevare i privilegi sul sistema.
    - **screenshot**: Tentativo di catturare schermate.
    - **win_registry**: Indica che il malware tenta di manipolare il registro di sistema di Windows.
    - **win_token**: Coinvolgimento nella gestione o alterazione dei token di sicurezza del sistema operativo, suggerendo la possibilità di impersonificazione o elevazione dei privilegi.
    - **win_files_operation**: Operazioni sui file, probabilmente per rubare informazioni o modificare file critici.

- **Conclusioni**: Dall'analisi statica, si evince che "AgentTesla.exe" è un malware con capacità di elevazione dei privilegi, manipolazione del sistema Windows e funzionalità di keylogging o raccolta di dati. Le regole Yara suggeriscono inoltre la raccolta di informazioni sensibili come token di sicurezza o credenziali di autenticazione.

## 2. Analisi Dinamica

L'analisi dinamica prevede l'esecuzione del malware in un ambiente controllato (come una sandbox) per osservarne il comportamento in tempo reale.




- **Comportamento del file**:
  - Durante l'esecuzione in **Cuckoo Sandbox**, il malware ha mostrato operazioni dannose:
    - **Escalation dei privilegi**: Confermato tramite le firme Yara, tentativi di ottenere accesso amministrativo.
    - **Cattura di schermate**: Tentativo di catturare schermate dal sistema infetto, il che implica la possibilità di spionaggio o monitoraggio del comportamento dell'utente.
    - **Accesso al registro di sistema**: Il malware tenta di leggere e/o scrivere chiavi di registro, possibilmente per modificare configurazioni di sicurezza o raccogliere dati sensibili.
    - **Manipolazione dei token di sicurezza**: Indicativo di attività volte ad alterare i privilegi degli utenti autenticati.
- **Tentativi di rilevazione di VM**: Durante l'esecuzione, il malware ha mostrato tentativi di identificare la presenza di una macchina virtuale (VM). Ha controllato la quantità di memoria disponibile e verificato la dimensione del disco, indicatori tipici utilizzati dai malware per evitare analisi in ambienti di test.

- **Rilevamento Antivirus**:
  - Il file è stato identificato come **malware** da 26 motori antivirus su **VirusTotal**, con rilevazioni che lo classificano principalmente come un **HackTool**, specificatamente il tool **AgentTesla**, noto per essere utilizzato per spiare e rubare informazioni personali tramite keylogging e sottrazione di credenziali.
  - Alcuni degli antivirus che hanno rilevato il malware includono BitDefender, McAfee, Sophos, eTrendMicro, che lo classificano come **Application.HackTool.BEL** o **Trojan.Win32.Negasteal**.
- **Azioni eseguite**:
  - Accesso al filesystem, come evidenziato dai numerosi tentativi di leggere e scrivere nella cartella **C:\Program Files (x86)**.
  - Tentativi di connessione remota: Non sono stati rilevati contatti con host esterni durante l'analisi dinamica, ma questo potrebbe essere dovuto al fatto che il malware attenda determinate condizioni per iniziare le comunicazioni.

**Conclusioni**

Dall'analisi combinata, "AgentTesla.exe" risulta essere un malware avanzato con capacità di spionaggio, esfiltrazione di dati e manipolazione del sistema. Le sue caratteristiche principali includono:

- Keylogging, cattura di schermate e raccolta di credenziali.
- Manipolazione del registro e dei token di sicurezza del sistema Windows.
- Rilevamento della presenza di macchine virtuali per evitare l'analisi.

È fortemente raccomandato di evitare l'esecuzione di questo file in ambienti non controllati, dato che potrebbe causare gravi danni e compromettere informazioni sensibili.