REPORT S9/L2: Analisi Malware (notepad-classico.exe)

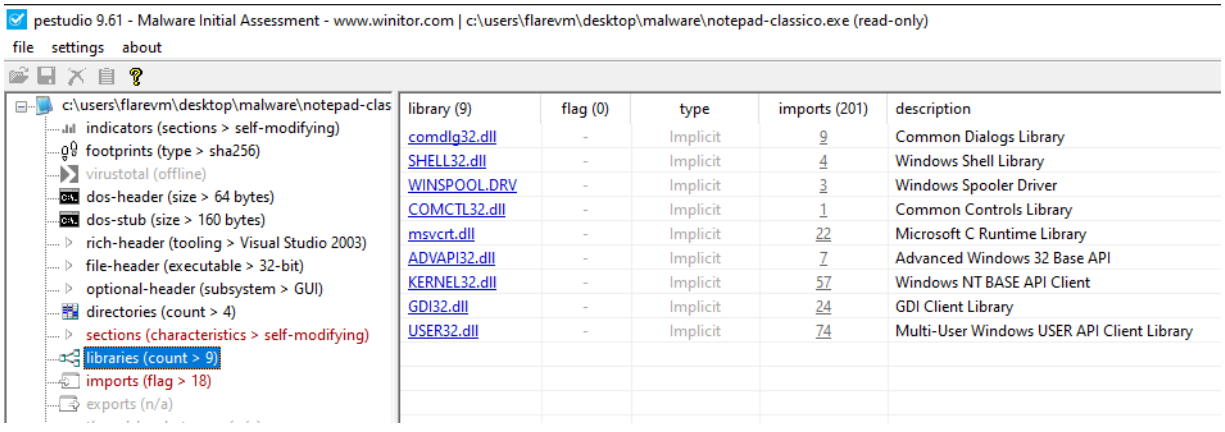
Oggetto: Analisi statica e dinamica del campione "notepad-classico.exe".
Strumenti Utilizzati: PEStudio, Tria.ge Sandbox.

---

1. Analisi Statica: Librerie Importate

Dall'analisi con PEStudio, il malware importa diverse librerie di sistema (DLL). Di seguito la descrizione tecnica delle principali librerie individuate e il loro potenziale utilizzo malevolo:

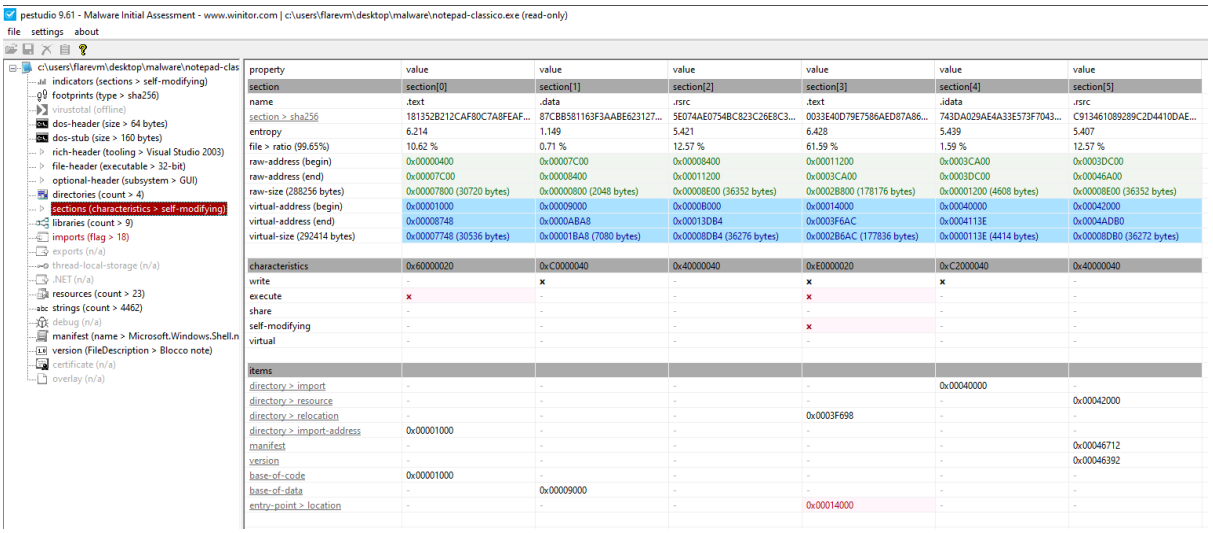
- **KERNEL32.dll**: È la libreria fondamentale di Windows. Gestisce la memoria, i processi e l'I/O.
    - *Analisi:* Essenziale per qualsiasi programma. Nei malware viene usata per creare nuovi processi, manipolare file o caricare altre DLL maligne.
- **ADVAPI32.dll (Advanced Windows 32 Base API)**: Gestisce il registro di sistema, i servizi e la sicurezza (account utenti).
    - *Analisi:* Sospetta. Spesso usata dai malware per ottenere persistenza (modificando le chiavi di registro per avviarsi all'accensione) o per creare servizi nascosti.
- **USER32.dll**: Gestisce l'interfaccia utente (finestre, mouse, tastiera).
    - *Analisi:* Sebbene legittima per un "Notepad", viene spesso abusata dai Keylogger per intercettare i tasti premuti (Hooking).
- **SHELL32.dll**: Consente l'accesso alle funzionalità della shell di Windows.
    - *Analisi:* Usata per eseguire comandi shell o aprire altri file/programmi (***ShellExecute***).
- **WINSPOOL.DRV**: Libreria per la gestione delle stampanti.
    - *Analisi:* Insolita per un semplice malware, ma potrebbe essere presente perché il malware è stato "iniettato" dentro un software legittimo che usava la stampa, oppure è una tecnica di distrazione.
- **GDI32.dll**: Gestione della grafica.
    - *Analisi:* Usata legittimamente per disegnare finestre, ma utilizzata dagli spyware per catturare screenshot dello schermo della vittima.



2. Analisi Statica: Sezioni del Malware

L'analisi dell'header PE mostra le sezioni in cui è diviso il codice del programma:

- **Section .text**: Contiene le istruzioni eseguibili (il codice vero e proprio del programma).
    - *Nota:* L'entropia è 6.214. Un valore medio-alto che suggerisce una densità di codice elevata, ma probabilmente non è pesantemente "impacchettato" (packed) in questa sezione specifica.
- **Section .data**: Contiene le variabili globali inizializzate e i dati statici.
    - *Nota:* Qui vengono spesso salvate stringhe come indirizzi IP del server C2 o messaggi di errore.
- **Section .rsrc (Resource)**: Contiene risorse come icone, immagini, menu e version info.
    - *Nota:* Un malware che si finge "Notepad" userà questa sezione per contenere l'icona legittima del blocco note per ingannare l'utente.
- **Section .idata**: Contiene la Import Address Table (IAT), ovvero l'elenco delle funzioni importate dalle DLL descritte al punto 1.



3. Analisi Dinamica (Report Tria.ge)

Il campione è stato eseguito nella sandbox Tria.ge per osservarne il comportamento reale.

Comportamento di Rete (Network)

L'indicatore più critico emerge dal traffico di rete. Il malware tenta una connessione diretta verso un indirizzo IP privato:

- **Destinazione:** ***192.168.50.100*** sulla porta **9001** (TCP).
- **Significato:** L'IP ***192.168.50.100*** è tipicamente l'indirizzo della macchina "Attaccante" (es. Kali Linux) in un ambiente di laboratorio virtuale. La porta **9001** non è standard per il traffico web, ma è comunemente usata per le **Reverse Shell** (connessioni di controllo remoto).
- Il malware tenta anche connessioni verso domini Google ***(c.pki.goog***), probabilmente per verificare la connessione internet.

Attività sul Sistema

- **File System:** Il malware viene eseguito dalla cartella temporanea ***AppData\Local\Temp***, comportamento tipico dei dropper.
- **Discovery:** Il report segnala "**System Location Discovery**", indicando che il malware controlla la lingua o la regione del sistema operativo, probabilmente per decidere se attivarsi o meno.

---

4. Considerazioni Finali e Verdetto

Nonostante Tria.ge assegni un punteggio di rischio basso (3/10) — probabilmente perché la connessione verso l'IP privato 192.168.50.100 è fallita nell'ambiente cloud pubblico — l'analisi combinata rivela la natura maligna del file.

1. **Natura della Minaccia:** Il file ***notepad-classico.exe*** è quasi certamente un **Payload Reverse TCP** generato da strumenti come ***Metasploit***.
2. **Tecnica:** Mascheramento (***Trojan***). Usa nome e probabilmente icona di un software legittimo (***Notepad***) per indurre l'utente all'esecuzione.
3. **Obiettivo:** Stabilire una connessione inversa verso l'attaccante (***IP 192.168.50.100***) per garantire accesso remoto al sistema vittima.
4. **Conclusione:** Il file è **MALEVOLO**. La presenza di connessioni in uscita verso IP privati su porte non standard è un chiaro indicatore di compromissione (IoC).