Malware Analysis Report

File: `notepad-classico.exe`
Analista: gianluca agostini
Date: 11/09/2025
macchina: Flare VM su VirtualBox (ambiente isolato)

---

1. Executive Summary

Durante l'analisi è stato esaminato l'eseguibile **`notepad-classico.exe`**, che si presenta come un normale Blocco Note di Windows. In realtà il file nasconde comportamenti sospetti, in particolare la creazione di connessioni TCP verso un host esterno e un accesso frequente a chiavi di registro legate all'input utente. Non sono stati trovati meccanismi di persistenza. Il campione risulta essere un potenziale **trojan backdoor con funzioni spyware (keylogger + C2)**.

2.Metodologia di Analisi

2.1 Verifica con VirusTotal

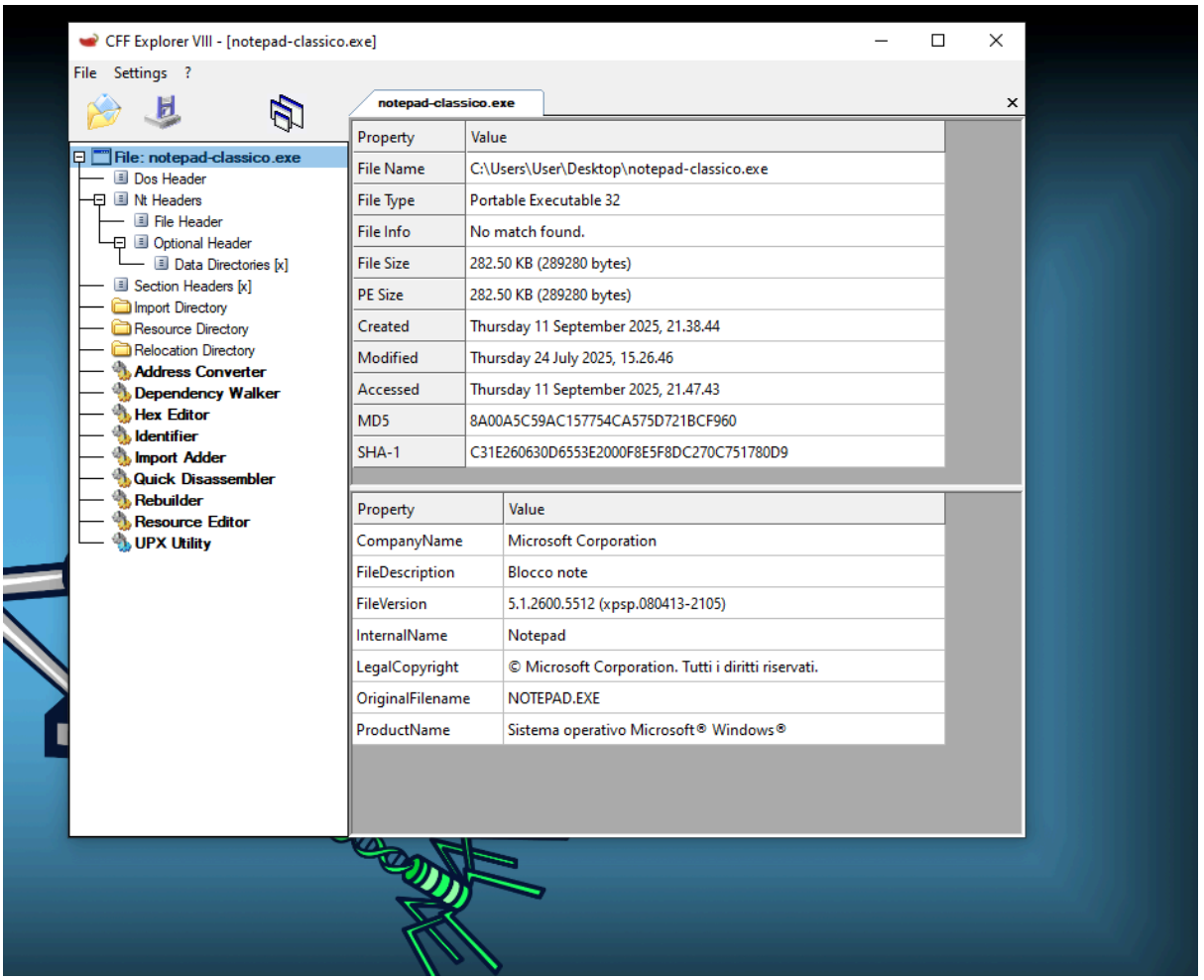
- Il campione è stato caricato su **VirusTotal**.
- Risultato: segnalazioni multiple da parte di antivirus, conferma che il file è classificato come malware e trojan,backdoor

2.2 Analisi Statica con CFF Explorer

- Verifica dell'intestazione PE → dichiarato come **`NOTEPAD.EXE`, Company `Microsoft Corporation`.**

- Sezioni normali **(`.text`, `.data`, `.rsrc`)** → nessun packer rilevato.

- Import di API sensibili **(`kernel32`, `user32`, `advapi32`)** → indizio di funzioni avanzate.

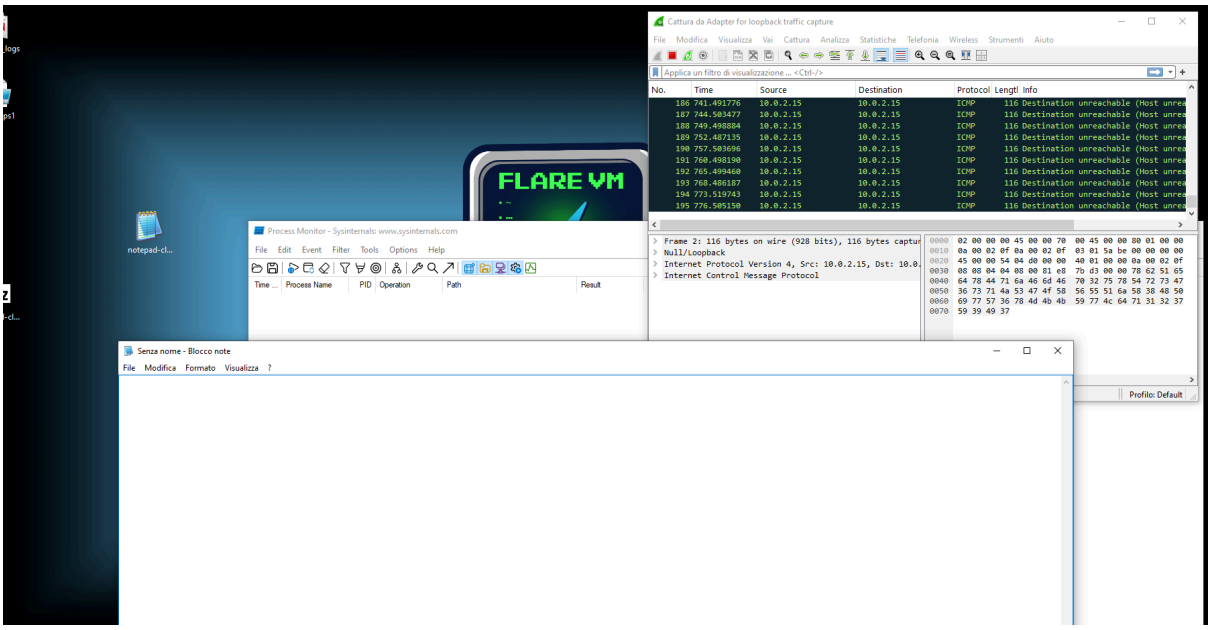


2.3 Monitoraggio Rete con Wireshark+process monitr

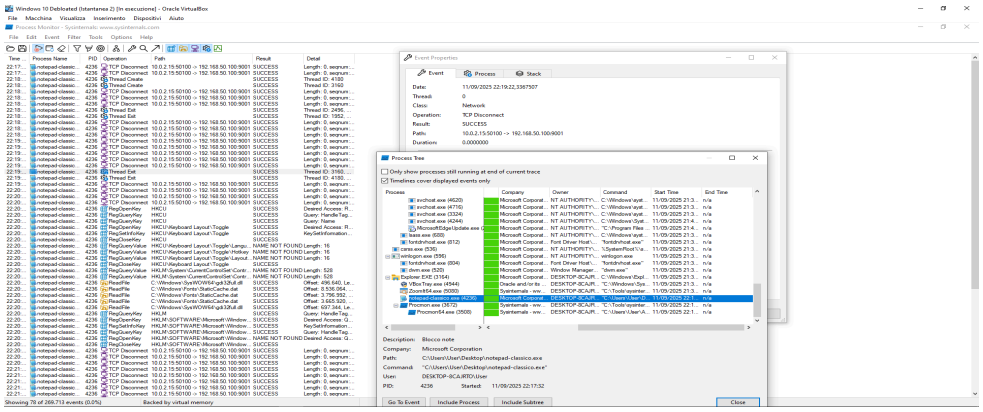
- Prima esecuzione sotto monitoraggio Wireshark → inizialmente nessun traffico anomalo.

- Successivamente, rilevati tentativi di connessione TCP sospetti verso indirizzo interno 192.168.50.100 porta 9001.

- Prima esecuzione bloccata: il programma non mostrava eventi significativi (possibile evasione anti-monitor).



2.4 avvio senza app avviate

- Dopo aver disabilitato altri processi e riavviato(usato il filtro di process monitor), il file ha mostrato attività molto più evidenti:
    - Accesso intensivo al **registro di sistema** quando scrivevo all'interno(HKLM\SYSTEM e HKCU\Software).
    - Creazione di thread multipli.
    - Connessioni **TCP verso 192.168.50.100:9001**, comportamento compatibile con un **reverse shell**.
    - il malware in più si infilava in un eseguibile come explorer
    - 

2.5 Persistenza con Autoruns

- Verifica dei punti di avvio automatico (Run, RunOnce, Winlogon, servizi).
- Nessuna voce sospetta rilevata.
- Conclusione: il malware **non sopravvive al riavvio**.

3. Risultati Osservati

- **Comportamento locale:** si avvia come finto Notepad e funziona anche come editor di testo per nascondere la sua natura.
- **Registro:** numerose query su chiavi legate a configurazioni di Windows e input utente.
- **Rete:** stabilisce connessioni TCP ricorrenti verso **`192.168.50.100:9001`.**
- **Persistenza:** assente.

---

4. Indicatori di Compromissione (IoC)

- **File:** `notepad-classico.exe`
- **Hash MD5:** `89A0C95AC175C5A07C6C89D0F72C7F18D0`
- **Connessioni:**
  - Origine: `10.0.2.15` (VM NAT)
  - Destinazione: `192.168.50.100:9001`
- **Processo:** `notepad-classico.exe` (PID 4236, figlio di Explorer.exe)

---

5. Conclusioni

Il file analizzato si comporta come un **trojan** mascherato da programma legittimo. È progettato per:

1. **Infiltrarsi senza destare sospetti** (mostrandosi come Notepad).
2. **Aprire connessioni verso un server esterno** con modalità simili a un **reverse shell**.

3. **Operare senza persistenza**, probabilmente per eludere controlli statici su riavvio.

---

6. Raccomandazioni

- Non eseguire mai il file su host reale.
- Monitorare la rete per eventuali tentativi di connessione alla porta **9001**.
- Usare sandbox dedicate (Cuckoo Sandbox o CAPE) per approfondire il comportamento.
- Aggiungere gli IoC in un sistema di detection aziendale (SIEM/SOC).

---

7. Conclusion

Il file **`notepad-classico.exe`** è un eseguibile malevolo che tenta di camuffarsi come Notepad legittimo. Durante l'esecuzione stabilisce connessioni TCP verso un host remoto e mostra comportamenti tipici da spyware, inclusa l'interazione con l'input dell'utente. Non implementa meccanismi di persistenza, il che lo rende meno pericoloso in termini di sopravvivenza sul sistema, ma comunque capace di attività malevole fintanto che rimane in esecuzione.