

Esercizio di Pratica S9L2 – Esercizio Malware

Sergio Falcone

INTRODUZIONE

Dato il file eseguibile: notepad-classico.exe (password: infected):

- Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse tramite AI;
- Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa tramite AI.

Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte ed elaborate con AI.

- Analisi Dinamica: Eseguire il malware in un ambiente controllato per osservare il suo comportamento e identificare le sue azioni in tempo reale.

PREFAZIONE

L'esercizio si svolgerà all'interno della Macchina Virtuale **FlareVM**, Sistema Operativo Windows10, in laboratorio controllato.

Tratta l'analisi del file eseguibile **notepad-classico.exe** attraverso strumenti quali, **CFF Explorer e Process Monitor**.

Sarà effettuata una ulteriore analisi attraverso Tria.ge

ESECUZIONE: CFF EXPLORER

(Analisi Statica)

Dall'analisi del file **notepad-classico.exe** attraverso **CFF Explorer** si sono ricavati i seguenti **Hash**:

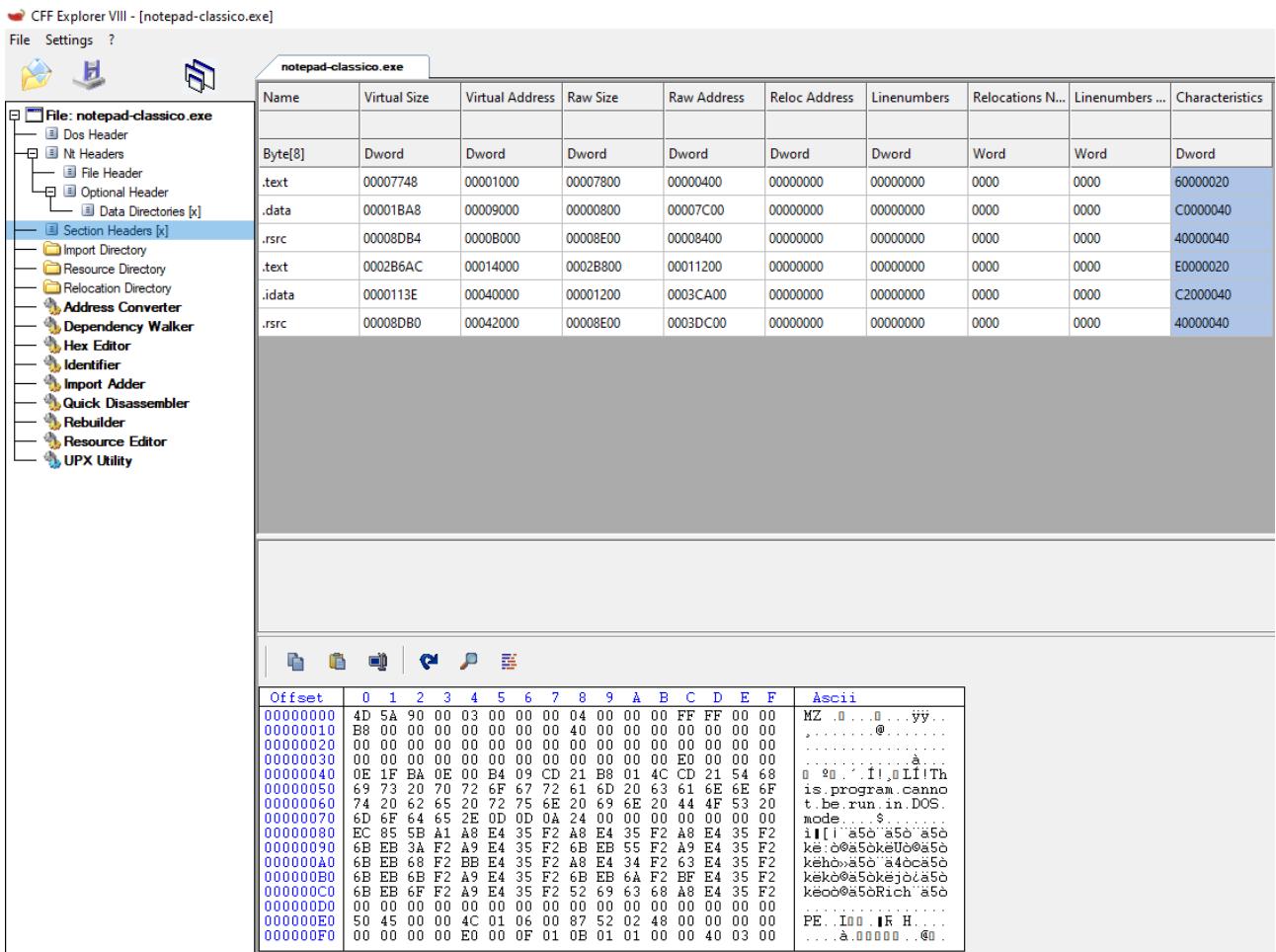
SHA256:

D2E6C9F9273663F3218BCD7CBFB3B6F599FBCE7A4BA986F9BBFF77E360
3988F2

MD5:

6FE25ED74B214298E440BDB980709C44

Visualizzazione di “Section Headers (x)”



Questa riguarda la struttura interna del file e come viene mappato in memoria
In questa struttura troviamo 2 sezioni .text e 2 sezioni .rsrc.

Solitamente, un file ha una sola sezione .text (codice) e una sola .rsrc (risorse). La presenza di duplicati suggerisce che il file sia stato modificato e/o unito a un altro eseguibile. Nella seconda sezione .text (riga 4), la **Characteristics** è **E0000020**. Il prefisso **E** significa che la sezione è **Read, Write ed Execute**.

.text: Contiene le istruzioni base del Notepad. È di sola lettura ed esecuzione (60000020).

.data: Qui risiedono le variabili globali. Essendo dati che il programma deve poter modificare, ha il permesso di scrittura (C0000040 = Read + Write).

.rsrc (Risorse): Contiene icone, cursori e stringhe dell'interfaccia. Di solito è di sola lettura (40000040).

.text (Estraneo): Permessi E0000020 (Read/Write/Execute), contiene del codice malevolo che viene spacchettato e iniettato all'avvio.

.idata: Tabella degli import. Fondamentale per collegare il codice alle DLL di sistema

.rsrc: Aggiunta di risorse, probabilmente necessaria per il codice contenuto nella seconda sezione **.text**.

Visualizzazione di “Import Directory”						
Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
comdlg32.dll	9	000400C8	00000000	FFFFFF	00040410	000012C4
SHELL32.dll	4	000400F0	00000000	FFFFFF	000404B5	00001174
WINSPOOL.DRV	3	00040104	00000000	FFFFFF	00040502	000012B4
COMCTL32.dll	1	00040114	00000000	FFFFFF	00040543	00001020
msvcrt.dll	22	0004011C	00000000	FFFFFF	00040566	000012EC
ADVAPI32.dll	7	00040178	00000000	FFFFFF	0004068A	00001000
KERNEL32.dll	57	00040198	00000000	FFFFFF	0004070F	0000108C
GDI32.dll	24	00040280	00000000	FFFFFF	00040AF1	00001028
USER32.dll	74	000402E4	00000000	FFFFFF	00040C5F	00001188

Dall'immagine precedente notiamo che vengono importate 9 Librerie, moduli fondamentali per la comprensione del Programma.

A seguire viene esposta la loro analisi.

- **comdlg32.dll (9 importazioni):** Gestisce le "Common Dialogs", ovvero le finestre standard di Windows per aprire, salvare file e scegliere i font.
- **SHELL32.dll (4 importazioni):** Fornisce l'accesso alle funzioni della shell di Windows
- **WINSPOOL.DRV (3 importazioni):** Gestisce l'interfaccia con il servizio di spooler di stampa.

- **COMCTL32.dll (1 importazione):** Fornisce controlli grafici avanzati
- **msvcrtdll.dll (22 importazioni):** La libreria runtime di Microsoft C per funzioni base di programmazione.
- **ADVAPI32.dll (7 importazioni):** Gestisce l'API di sicurezza avanzata, inclusi i permessi e il Registro di sistema.
- **KERNEL32.dll (57 importazioni):** La libreria vitale per la gestione della memoria, dei processi e dei file.
- **GDI32.dll (24 importazioni):** Motore grafico per disegnare testo e immagini elementari.
- **USER32.dll (74 importazioni):** Responsabile della creazione delle finestre e dei menu.

ESECUZIONE: PROCESS MONITOR

(Analisi Dinamica)

PREMESSA: Questo è un laboratorio controllato, sono state effettuate i giusti accorgimenti per poter eseguire il programma in sicurezza.

Si osserva il programma mentre è in esecuzione

Time ...	Process Name	PID	Operation	Path	Result	Detail
6:00:1...	notepad-classic...	3304	TCP Disconnect	10.0.2.15.49771 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum:....
6:00:2...	notepad-classic...	3304	RegQueryKey	HKEY_LOCAL_MACHINE\...	SUCCESS	Query: HandleTag...
6:00:2...	notepad-classic...	3304	RegQueryKey	HKEY_LOCAL_MACHINE\...	SUCCESS	Query: Name
6:00:2...	notepad-classic...	3304	RegOpenKey	HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Run\{...	REPARSE	Desired Access: Q...
6:00:2...	notepad-classic...	3304	RegOpenKey	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\{...	SUCCESS	Desired Access: Q...
6:00:2...	notepad-classic...	3304	RegSetInfoKey	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\{...	SUCCESS	KeySetInformation...
6:00:2...	notepad-classic...	3304	RegQueryValue	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\{...	SUCCESS	NAME NOT FOUND Length: 16
6:00:2...	notepad-classic...	3304	RegCloseKey	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\{...	SUCCESS	
6:00:2...	notepad-classic...	3304	RegQueryKey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\{...	SUCCESS	Query: HandleTag...
6:00:2...	notepad-classic...	3304	RegQueryKey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\{...	SUCCESS	Query: Name
6:00:2...	notepad-classic...	3304	RegOpenKey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\{...	SUCCESS	Desired Access: Q...
6:00:2...	notepad-classic...	3304	RegSetInfoKey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\{...	SUCCESS	KeySetInformation...
6:00:2...	notepad-classic...	3304	RegQueryValue	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\{...	SUCCESS	NAME NOT FOUND Length: 16
6:00:2...	notepad-classic...	3304	RegCloseKey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\{...	SUCCESS	
6:00:2...	notepad-classic...	3304	TCP Disconnect	10.0.2.15.49771 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum:....
6:00:3...	notepad-classic...	3304	Thread Create		SUCCESS	Thread ID: 5540
6:00:3...	notepad-classic...	3304	Thread Create		SUCCESS	Thread ID: 6644
6:00:3...	notepad-classic...	3304	TCP Disconnect	10.0.2.15.49771 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum:....
6:00:4...	notepad-classic...	3304	TCP Disconnect	10.0.2.15.49771 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum:....
6:00:5...	notepad-classic...	3304	TCP Disconnect	10.0.2.15.49771 -> 192.168.50.100:9001	SUCCESS	Length: 0, seqnum:....

Analisi degli Eventi

- **Connessioni di Rete (TCP Disconnect):** Si vedono tentativi di connessione verso l'IP 192.168.50.100 sulla porta 9001. Un normale blocco note non dovrebbe comunicare in rete, specialmente su porte spesso associate a **Reverse Shell** o Command & Control (C2).
- **Accesso al Registro (RegQueryKey/RegOpenKey):** Il processo sta interrogando chiavi di registro in HKLM (Local Machine) e HKCU (Current User). Sta cercando informazioni sulla configurazione del sistema o tentando di stabilire una "persistenza".
- **Creazione di Thread (Thread Create):** Il processo genera nuovi thread (ID 5540, 6644), indicando che sta eseguendo operazioni multitasking, probabilmente per gestire la comunicazione di rete in background mentre l'utente vede l'interfaccia del blocco note.

Conclusioni:

- È stato preso un eseguibile legittimo (**notepad.exe**).
- È stata aggiunta una nuova sezione (la seconda **.text**) contenente del codice malevolo (**shellcode**).
- I permessi della sezione sono stati impostati su **E0000020** per permettere al codice di auto-modificarsi o eseguirsi.
- All'avvio, il programma "finge" di essere un editor, ma contemporaneamente apre una connessione verso l'**IP 192.168.50.100**.

ESECUZIONE: TRIA.GE

L'analisi attraverso Tria.ge valuta il seguente Malware con un punteggio di 3/10.
La sua attività è di Discovery.

Estratto del file pdf di Triage (Screenshots)

Part 4. Analysis: behavioral1

4. 1. Detonation Overview

Target notepad-classico.exe	SHA256 d2e6c9f9273663f3218bcd7cbfb3b6f599fbce7a4ba986f9bbff77e3603988f2	Filesize 282KB
Submitted 2026-02-03 15:21	Reported 2026-02-03 15:24	Platform win10v2004-20260130-en

4. 2. Command Line

"C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe"

4. 3. Signatures

System Location Discovery: System Language Discovery

Discovery	Indicator	Process	Target
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NLS\Language	C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe	N/A

4. 4. Processes

C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe
"C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe"

4. 5. Network

Country	Destination	Domain	Proto
N/A	192.168.50.100:9001		tcp
US	8.8.8.53	g.bing.com	udp
US	150.171.28.10:443	g.bing.com	tcp
SE	80.239.150.33:443	www.bing.com	tcp
SE	80.239.150.33:443	www.bing.com	tcp
US	8.8.8.53	c.pki.goog	udp
GB	142.251.29.94:80	c.pki.goog	tcp

4. 6. Files

memory/3600-0-0x0000000001000000-0x000000000104ADB0-memory.dmp

memory/3600-1-0x0000000000EC0000-0x0000000000EF1000-memory.dmp

memory/3600-5-0x0000000001000000-0x000000000104ADB0-memory.dmp

Part 5. Analysis: behavioral

5. 1. Detonation Overview

Target notepad-classico.exe	SHA256 d2e6c9f9273663f3218bcd7cbfb3b6f599fbce7a4ba986f9bbff77e3603988f2	Filesize 282KB
Submitted 2026-02-03 15:21	Reported 2026-02-03 15:24	Platform win11-20260130-en
		Max time kernel 149s

5. 2. Command Line

```
"C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe"
```

5. 3. Signatures

System Location Discovery: System Language Discovery			
Description	Indicator	Process	Target
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NLS\Language	C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe	N/A

5. 4. Processes

```
C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe
"C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe"
```

5. 5. Network

Country	Destination	Domain	Proto
N/A	192.168.50.100:9001		tcp
US	150.171.27.10:443	tse1.mm.bing.net	tcp
US	150.171.27.10:443	tse1.mm.bing.net	tcp
US	150.171.27.10:443	tse1.mm.bing.net	tcp
US	150.171.27.10:443	tse1.mm.bing.net	tcp
US	150.171.27.10:443	tse1.mm.bing.net	tcp
GB	142.251.29.94:80	c.pki.goog	tcp

5. 6. Files

```
memory/5208-0-0x0000000001000000-0x000000000104ADB0-memory.dmp
```

```
memory/5208-1-0x0000000000D60000-0x0000000000D91000-memory.dmp
```

```
memory/5208-5-0x0000000001000000-0x000000000104ADB0-memory.dmp
```

Le sezioni mostrate, **Part 4** e **Part 5** descrivono i risultati dell'**analisi comportamentale** (behavioral) eseguita in due ambienti virtuali differenti: **Windows 10** (Part 4) e **Windows 11** (Part 5).

Analisi Comportamentale 1 (Windows 10) Part 4

In questa sezione, il file è stato eseguito su una macchina **Windows 10** e il sistema ha contrassegnato l'attività come "**Discovery**" (Scoperta). Nello specifico, il programma ha cercato di identificare la lingua del sistema accedendo alle chiavi di registro (`\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NLS\Language`)

Il file è stato eseguito dal percorso temporaneo
(`C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe`)

Sono state rilevate diverse connessioni:

- Una connessione sospetta verso un IP locale/privato **192.168.50.100** sulla porta **9001**.
- Traffico verso domini legittimi come **bing.com** e **pki.goog** (Google)

Analisi Comportamentale 2 (Windows 11)

Questa sezione ripete il test su una macchina Windows 11 per verificare se il comportamento cambia a seconda del sistema operativo.

Si nota che anche in Windows 11, il programma ha eseguito il "System Language Discovery" interrogando le stesse chiavi di registro.

Oltre alla connessione all'**IP 192.168.50.100:9001**, sono stati registrati numerosi contatti verso **tse1.mm.bing.net**