

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.

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, 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:

D2E6C9F9273663F3218BCD7CBFB3B6F599FBCE7A4BA986F9BBFF77E360398
8F2

MD5:
6FE25ED74B214298E440BDB980709C44

Visualizzazione di “Section Headers (x)”

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Bye[8]	Dword	Dword	Dword	Dword	Dword	Word	Word		Dword
.text	00007748	00001000	00007800	00000400	00000000	00000000	0000	0000	60000020
.data	00001BA8	00009000	00000800	00007C00	00000000	00000000	0000	0000	C0000040
.rsrc	00008DB4	0000B000	00008E00	00008400	00000000	00000000	0000	0000	40000040
.text	0002B6AC	00014000	0002B800	00011200	00000000	00000000	0000	0000	E0000020
.idata	0000113E	00040000	00001200	0003CA00	00000000	00000000	0000	0000	C2000040
.rsrc	00008DB0	00042000	00008E00	0003DC00	00000000	00000000	0000	0000	40000040

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	90	00	03	00	00	04	00	00	FF	FF	00	00	MZ	..@...yy..	
00000010	B0	00	00	00	00	00	00	40	00	00	00	00	00	00	00@.....	
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00@.....	
00000030	00	00	00	00	00	00	00	00	00	00	E0	00	00	00	00@.....	
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	94	68@.....
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6F	is.program.canno	t.be.run.in.DOS
00000060	74	20	62	65	20	72	75	6E	20	59	6E	20	44	4F	93	20@.....
00000070	6D	6F	64	65	2B	0D	0D	0A	24	00	00	00	00	00	00	00	mode....\$.....
00000080	EC	85	5B	A1	A8	E4	35	F2	A8	E4	35	F2	11[1`á5óá5óá5ó	á5ó	á5ó	á5ó	á5ó
00000090	6B	EE	3A	F2	A9	E4	35	F2	6B	EE	55	F2	A9	E4	35	F2	ké:@á5ókeUóá5ó
000000A0	6B	EE	68	F2	BE	E4	35	F2	A8	E4	34	F2	63	E4	35	F2	kéhó:á5óá4óccá5ó
000000B0	6B	EE	6B	F2	A9	E4	35	F2	6B	EE	6A	F2	BF	E4	35	F2	kékó@á5ókejó:á5ó
000000C0	6B	EE	6F	F2	A9	E4	35	F2	52	69	63	68	A8	E4	35	F2	kéod@á5óRich'á5ó
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00@.....
000000E0	50	45	00	00	4C	01	06	00	87	52	02	48	00	00	00	00	PE...IRH....
000000F0	00	00	00	00	E0	00	0F	01	0B	01	01	00	40	03	00	00à.00000..@..

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”						
notepad-classico.exe						
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
- **msvcrt.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

Process Monitor - Sysinternals: www.sysinternals.com						
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	HKLM	SUCCESS	Query: HandleTag...
6:00:2...	notepad-classic...	3304	RegQueryKey	HKLM	SUCCESS	Query: Name
6:00:2...	notepad-classic...	3304	RegOpenKey	HKLM\Software\WOW6432Node\Mic...	REPARSE	Desired Access: Q...
6:00:2...	notepad-classic...	3304	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: Q...
6:00:2...	notepad-classic...	3304	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	KeySetInformation...
6:00:2...	notepad-classic...	3304	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 16
6:00:2...	notepad-classic...	3304	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
6:00:2...	notepad-classic...	3304	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
6:00:2...	notepad-classic...	3304	RegQueryKey	HKCU	SUCCESS	Query: Name
6:00:2...	notepad-classic...	3304	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: Q...
6:00:2...	notepad-classic...	3304	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	KeySetInformation...
6:00:2...	notepad-classic...	3304	RegQueryValue	HKCU\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 16
6:00:2...	notepad-classic...	3304	RegCloseKey	HKCU\SOFTWARE\Microsoft\Window...	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:...

Showing 20 of 182,095 events (0.010%) Backed by virtual memory

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					
Description	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	8.8.8.8:53	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	8.8.8.8:53	c.pki.goog	udp
GB	142.251.29.94:80	c.pki.goog	tcp

4. 6. Files

memory/3600-0-0x00000000001000000-0x0000000000104ADB0-memory.dmp
memory/3600-1-0x0000000000EC0000-0x0000000000EF1000-memory.dmp
memory/3600-5-0x00000000001000000-0x0000000000104ADB0-memory.dmp

Part 5. Analysis: behavioral2

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				
discovery				
Description	Indicator	Process	Target	
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\IN LS\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/5208-1-0x000000000D60000-0x000000000D91000-memory.dmp
```

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