

# W21D4 – Pratica

Epic Education Srl

**Analisi statica malware notepad-classico.exe**

**Considerazioni finali sul malware**

Simone Giordano

02/12/2025



## Contatti:

Tel: 3280063044

Email: [mynameisimone@gmail.com](mailto:mynameisimone@gmail.com)

Linkedin: <https://www.linkedin.com/in/simone-giordano-91290652/>

## Sommario

<b>Analisi statica malware notepad-classico.exe.....</b>	<b>3</b>
Analisi librerie .....	3
Sezioni del malware .....	4
<b>Considerazioni finali sul malware Esercizio facoltativo.....</b>	<b>6</b>

# Analisi statica malware notepad-classico.exe

## Analisi librerie

**TRACCIA:** Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse tramite AI;

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
msvcrtdll	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

Libreria	Descrizione
comdlg32.dll	Gestisce le finestre standard come "Apri file", "Salva file", stampa, scelta colori e font.
SHELL32.dll	Fornisce funzioni del Windows Shell: aprire cartelle, lanciare programmi, gestire desktop e Explorer.
WINSPOOL.DRV	Gestisce la stampa: invio documenti alla stampante e gestione delle code di stampa.
COMCTL32.dll	Controlli grafici standard di Windows: pulsanti, liste, progress bar, toolbar, tab, slider.
msvcrtdll	Runtime del linguaggio C: funzioni per memoria, stringhe, input/output, matematica. Usata quasi sempre.
ADVAPI32.dll	Funzioni avanzate di Windows: registro di sistema, servizi Windows, permessi, log eventi.
KERNEL32.dll	La libreria centrale dei programmi: gestione processi, memoria, file, thread, moduli. Importata sempre.
GDI32.dll	Grafica 2D di Windows: testo, forme, immagini, rendering sullo schermo e stampante.

**USER32.dll**

Gestisce finestre e interfaccia utente: bottoni, input mouse/tastiera, messaggi di sistema.

## Sezioni del malware

**TRACCIA:** indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa tramite AI.

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
00000250	00000258	0000025C	00000260	00000264	00000268	0000026C	00000270	00000272	00000274
Byte[8]	Dword	Dword	Dword	Dword	Dword	Word	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

This section contains:  
Code Entry Point: 00014000  
Relocation Directory: 0003F698

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	60	68	31	40	01	01	FF	15	C8	10	00	01	68	3A	40	01	'h1@00j0E0..0:h:00
00000010	01	50	FF	15	10	11	00	01	8D	15	47	40	01	01	6A	00	0Py00000G00j.
00000020	6A	00	6A	00	52	6A	00	6A	00	FF	D0	61	E9	6C	33	FF	j..Rj.j.yBaé13y
00000030	EE	6B	65	72	6E	65	6C	33	32	00	43	72	65	61	74	65	ykernel32.Create
00000040	54	68	72	65	61	64	00	8D	15	4D	40	01	01	4D	5A	E8	Thread.0M@0MZé
00000050	00	00	00	00	SB	52	45	55	89	E5	81	C3	90	49	00	00	REUà Á I..
00000060	FF	D3	81	C3	69	68	02	00	53	6A	04	50	FF	D0	00	00	yó Áih.Sj0PyB..
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....0..0..0..
00000080	00	00	00	00	00	00	00	00	00	00	01	00	00	0E	1F	BA	0...!L!This.
00000090	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	69	73	20	program cannot.b
000000A0	70	72	6F	67	72	61	6D	20	63	61	6E	6E	74	20	62	e run in DOS mod	
000000B0	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	6D	6F	64	e...\$....üG%
000000C0	65	2E	0D	0D	0A	24	00	00	00	00	FB	47	25				
000000D0	39	BF	26	4B	6A	BF	26	4B	6A	BF	26	4B	6A	B2	74	AA	9é&Kjé&Kjé&Kjé&Kjé

Nome sezione	Virtual Address	Caratteristiche	Descrizione
Byte[8] / Header	0x00000000	Dword	Piccola sezione tecnica usata internamente dal loader. Non contiene codice.
.text (1ª)	0x00001000	0x60000020 (Executable + Readable)	Sezione <b>legittima</b> che contiene il codice macchina originale del programma (notepad-classico.exe). Qui dovrebbe esserci il codice Win32 normale.
.data	0x00008000	0xC0000040 (Readable + Writable)	Contiene dati globali e variabili usate dal programma legittimo. Tipica sezione dei programmi Windows.

.rsrc (1 <sup>a</sup> )	0x0000B000	0x40000040 (Readable)	Contiene risorse: icone, dialoghi, immagini, stringhe. Anche questa è una sezione <b>normale</b> .
.text (2 <sup>a</sup> ) — ⚡ MALEVOLE	0x00014000	0xE0000020 (Executable + Writable + Extra flags)	<b>Sezione aggiunta manualmente dal malware.</b> <b>Contiene shellcode.</b> Si vede codice che fa: push valori, chiamate indirette, importazione dinamica di API, stringhe offuscate e la stringa “kernel32.CreateThread”. Inoltre è eseguibile e <i>scrivibile</i> , caratteristica quasi sempre malevola. <b>L'Entry Point del file è stato reindirizzato qui</b> (0x00014000).
.idata	0x00028000	0xC2000040 (Readable + Writable)	Tavola delle importazioni (IAT). Qui il malware potrebbe aver aggiunto funzioni importate dinamicamente. È sospetta la presenza di flag scrivibile + eseguibile.

## Considerazioni finali sul malware

## Esercizio facoltativo

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

Analizzando il file **notepad-classico.exe** è emerso che due sezioni **.text** e **.rsrc** sono duplicate.

- La sezione .text duplicata contiene un'iniezione di codice.
  - La sezione .rsrc duplicata contiene dati di configurazione necessari al payload.
  - Contiene la firma MZ a indicare che si tratta di un file PE valido per camuffarsi.

Notiamo che nella sezione .text duplicata, contenente il codice malevolo, è presente una stringa di testo ws2\_32.dll che sarebbe una libreria contenente le funzioni di rete per Windows, quindi il file probabilmente fa operazioni di rete.

Section	Virtual Address	Size	File Address	Characteristics	Virtual Size	File Size	Entropy	Hash
.data	00000000	00000000	00000000	00000000	00000000	00000000	0000	C0000040
.zsrc	00000000	00000000	00000000	00000000	00000000	00000000	0000	40000040
.text	00000000	00014000	00000000	00000000	00011200	00000000	0000	E0000020
.idata	00000000	00040000	00000000	00000000	0003AC00	00000000	0000	C2000040
.zsrc	00000000	00042000	00000000	00000000	0003DC00	00000000	0000	40000040

This section contains:

Code Entry Point: 00014000  
Relocation Directory: 003JP698

Find String: ws2

Match Case    Unicode

Hex Find

Reset

Status: String found

## Analizzando meglio l'ASCII

- 1 - Apre una connessione a un server e scambia dati
  - 2 - Si comporta come un browser (chiama un sito, legge dati, forse invia qualcosa)
  - 3 - Protegge/cifra i dati

---

Ascii

## ASCII

## 1. WSADuplicateS

info. || freeaddr

nfo\_WS2\_32.dll

jectEx.B.CryptIm

portPublickeyInt  
9..F.CertGetCert

*ificateContextPr  
    *ssocut\_* CPWPT22.d*

Property.CRYPT132.dll.t.InternetCra

ckUrlW. . Internal  
tOpenW. k Internal

tCloseHandle.r.I

InternetReadF

1 -  1

ANSWER

ANSWER

Cercando tramite **SHA1 o MD5** su VirusTotal è emerso che 58 security vendor l'hanno segnalato come malevolo e riporta tutta una serie di informazioni, come i domini/IP contattati, il riassunto delle attività, le tecniche riportate dal MITRE e molto altro.

<https://www.virustotal.com/gui/file/d2e6c9f9273663f3218bcd7cbfb3b6f599fbce7a4ba986f9bbff77e3603988f2/behavior>

MD5: 8A00A5C59AC157754CA575D721BCF960  
SHA-1: C31E260630D6553E2000F8E5F8DC270C751780D9

d2e6c9f9273663f3218bcd7cbfb3b6f599fbce7a4ba986f9bbff77e3603988f2

58 / 72 security vendors flagged this file as malicious

Community Score

Reanalyze Similar More

d2e6c9f9273663f3218bcd7cbfb3b6f599fbce7a4ba986f9bbff77e3603988f2  
NOTEPAD.EXE  
peexe detect-debug-environment long-sleeps

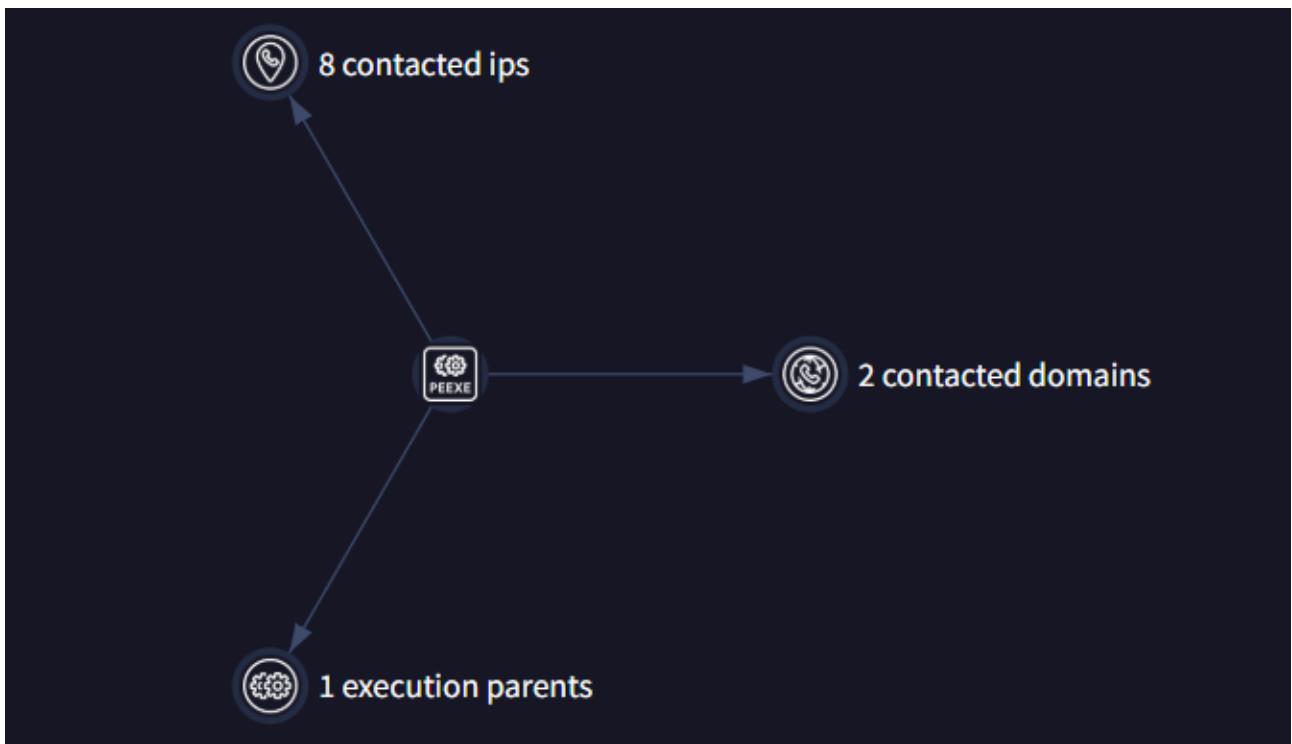
Size: 282.50 KB | Last Analysis Date: 12 days ago | EXE

### Contacted Domains (2)

Domain	Detections	Created	Registrar
res.public.onecdn.static.microsoft	1 / 95	2023-05-05	MarkMonitor Inc.
www.microsoft.com	0 / 95	1991-05-02	MarkMonitor Inc.

### Contacted IP addresses (8)

IP	Detections	Autonomous System	Country
151.101.22.172	0 / 95	54113	US
192.168.50.100	0 / 95	-	-
20.69.140.28	0 / 95	8075	US
20.99.133.109	0 / 95	8075	US
23.196.145.221	0 / 95	16625	US
23.46.228.41	0 / 95	20940	US
23.46.228.49	0 / 95	20940	US
23.55.140.42	0 / 95	16625	US



## Activity Summary

**⚠ 2 Detections**  
2 MALWARE   1 TROJAN

**Mitre Signatures**  
3 MEDIUM   1 LOW   17 INFO

**Behavior Tags** ⓘ  
detect-debug-environment   long-sleeps

**Dynamic Analysis Sandbox Detections** ⓘ

- ⚠ The sandbox CAPE Sandbox flags this file as: MALWARE
- ⚠ The sandbox Zenbox flags this file as: MALWARE TROJAN

