

## **UNIT3 S9/L2 - ANALISI STATICÀ + DINAMICA MALWARE**

---

Rispondere ai seguenti quesiti, con riferimento al file eseguibile notepad-classico.exe

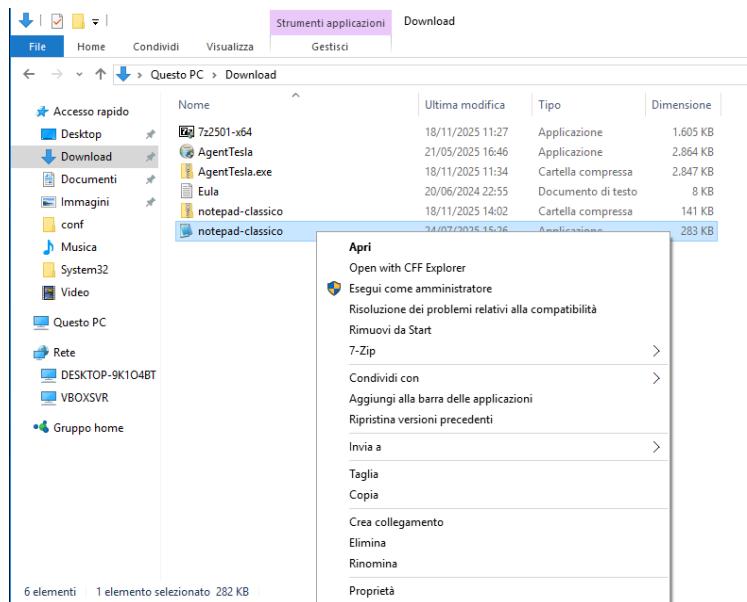
- *Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse tramite AI;*
- *Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa tramite AI.*

*opzionale:*

- *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.*
-

## Esercizio:

scarico il file notepad-classic.exe



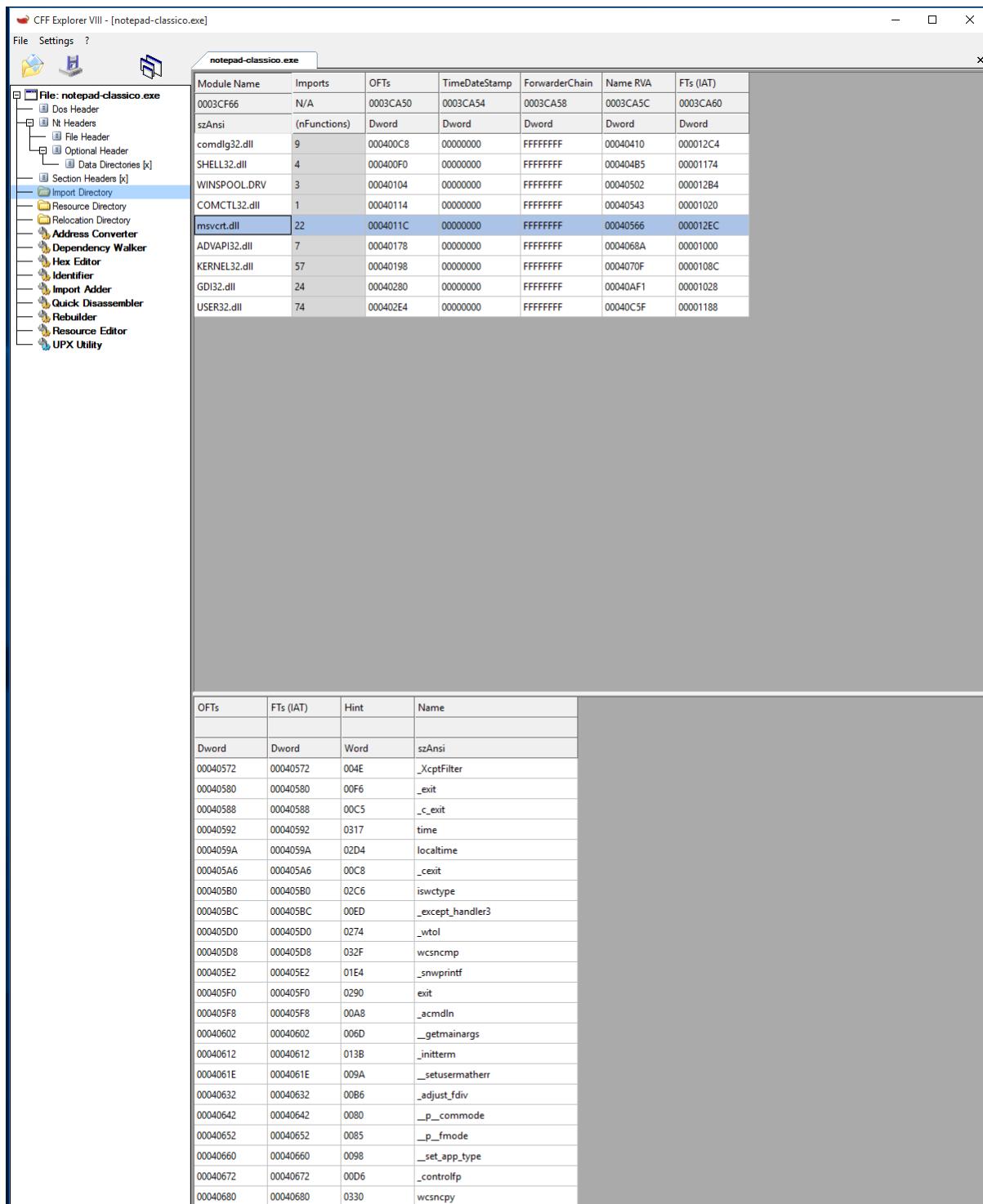
Per eseguire l'analisi statica apro il programma con CFF explorer.

la pagina iniziale presentata è la seguente:

The screenshot shows the CFF Explorer VIII interface. The left pane displays a tree view of the file structure for 'notepad-classic.exe', including sections like Dos Header, Nt Headers, and Resource Directory. The right pane displays two tables of properties for the file:

Property	Value
File Name	C:\Users\user\Downloads\notepad-classico.exe
File Type	Portable Executable 32
File Info	No match found.
File Size	282.50 KB (289280 bytes)
PE Size	282.50 KB (289280 bytes)
Created	Tuesday 18 November 2025, 14.03.31
Modified	Thursday 24 July 2025, 14.26.46
Accessed	Tuesday 18 November 2025, 14.03.31
MD5	8A00A5C59AC157754CA575D721BCF960
SHA-1	C31E260630D6553E2000F8E5F8DC270C751780D9

Property	Value
CompanyName	Microsoft Corporation
FileDescription	Blocco note
FileVersion	5.1.2600.5512 (xpsp.080413-2105)
InternalName	Notepad
LegalCopyright	© Microsoft Corporation. Tutti i diritti riservati.
OriginalFilename	NOTEPAD.EXE
ProductName	Sistema operativo Microsoft® Windows®



(è possibile vedere le **librerie importate** tramite “import directory”)

## KERNEL32.dll

- Funzione: È la libreria centrale e più essenziale di Windows (Core Kernel).
- Ruolo: Gestisce le funzioni fondamentali del sistema operativo, come l'allocazione e gestione della memoria, la creazione e sincronizzazione di processi e thread, e l'accesso di basso livello al file system e all'hardware.
- Significato per il Malware: È richiesta per qualsiasi operazione base, dalla semplice esecuzione di codice alla manipolazione avanzata dei processi.

---

## USER32.dll

- Funzione: Gestisce l'interfaccia utente (User Interface - UI).
  - Ruolo: Fornisce le API per la creazione e la gestione di finestre, menu, cursori, icone e per l'elaborazione degli input da mouse e tastiera.
  - Significato per il Malware: Utilizzata per interagire con il desktop, creare finestre nascoste o messaggi (anche per phishing), o intercettare l'input dell'utente (keylogging).
- 

## GDI32.dll

- Funzione: Gestisce le funzioni di interfaccia per dispositivi grafici (Graphics Device Interface).
  - Ruolo: Contiene le API per l'output grafico, permettendo al programma di disegnare sullo schermo, stampare documenti, gestire font e manipolare grafica bidimensionale.
  - Significato per il Malware: Raramente usata per la logica malevola pura, ma è necessaria se il malware deve visualizzare messaggi grafici, creare screenshot, o manipolare l'output grafico.
- 

## ADVAPI32.dll

- Funzione: Fornisce servizi di sicurezza avanzati e API di accesso al Registro.
  - Ruolo: Gestisce l'accesso e la manipolazione del Registro di sistema (per la persistenza), i servizi Windows, i diritti di sicurezza (es. token) e le funzionalità di crittografia.
  - Significato per il Malware: Essenziale per stabilire la persistenza (eseguirsi automaticamente all'avvio) scrivendo chiavi nel Registro, per elevare i privilegi o per utilizzare funzioni di crittografia e hashing.
- 

## SHELL32.dll

- Funzione: Gestisce le operazioni della shell di Windows.
  - Ruolo: Fornisce API per interagire con l'ambiente desktop, il file system e per eseguire programmi. Funzioni comuni includono ShellExecute (per lanciare altri eseguibili), la gestione delle cartelle speciali e delle icone.
  - Significato per il Malware: Usata per eseguire file, spostarsi nel file system, accedere a directory speciali o aprire URL.
- 

## msvcrt.dll

- Funzione: È la libreria di runtime del compilatore Microsoft Visual C++ (C RunTime Library).

- Ruolo: Implementa le funzioni standard del linguaggio C e C++, come la manipolazione delle stringhe (strcpy), le operazioni matematiche, l'input/output (printf/sccanf) e la gestione della memoria dinamica (malloc/free).
  - Significato per il Malware: Necessaria se il codice è stato scritto in C/C++ e utilizza funzioni standard.
- 

## COMDLG32.dll

- Funzione: Gestisce le finestre di dialogo comuni (Common Dialog Boxes).
  - Ruolo: Fornisce le API per visualizzare le finestre di dialogo standard di Windows, come la finestra "Apri File" (GetOpenFileName), "Salva File" o "Stampa".
  - Significato per il Malware: Potrebbe essere usata per cercare file sul sistema o per ingannare l'utente visualizzando finestre familiari.
- 

## COMCTL32.dll

- Funzione: Gestisce i controlli comuni (Common Controls Library).
  - Ruolo: Contiene le API per elementi di interfaccia utente più complessi e moderni, come barre di avanzamento, barre degli strumenti, schede e Tree View.
  - Significato per il Malware: Necessaria se il malware ha un'interfaccia utente grafica più elaborata (sebbene molti malware siano headless e non ne abbiano bisogno).
- 

## WINSPOOL.DRV

- Funzione: Driver e libreria di gestione dello spooler di stampa.
- Ruolo: Controlla l'accesso alle funzionalità di stampa e al servizio Print Spooler.
- Significato per il Malware: I malware che importano funzioni da WINSPOOL.DRV a volte lo fanno per sfruttare vulnerabilità nel servizio di spooler di stampa (storicamente sfruttato per l'elevazione dei privilegi, come in attacchi "PrintNightmare").

CFF Explorer VIII - [notepad-classico.exe]

File Settings ?

File : notepad-classico.exe

notepad-classico.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
000002A0	000002A8	000002AC	000002B0	000002B4	000002B8	000002BC	000002C0	000002C2	000002C4
Bytes[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

This section contains:

Resource Directory: 00042000

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....0.....0
00000010	03	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	P.....0.....0
00000020	05	00	00	00	00	B0	01	00	80	06	00	00	00	00	00	00	.....0.....6.....
00000030	09	00	00	00	D0	02	00	80	0E	00	00	00	00	20	03	00	80
00000040	10	00	00	00	00	00	00	00	00	04	00	00	00	00	00	00	.....F0.....0.....
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0000009000
00000060	03	00	00	00	A8	00	00	80	02	00	00	00	C0	00	00	80	.....0.....A.....
00000070	03	00	00	00	D8	00	00	80	04	00	00	00	F0	00	00	80	.....0.....8.....
00000080	05	00	00	00	00	01	00	80	06	00	00	00	20	01	00	80	.....0.....F0.....
00000090	07	00	00	00	38	01	00	80	08	00	00	00	50	01	00	80	.....0.....0.....
000000A0	00	00	00	00	68	01	00	80	00	00	00	00	00	00	00	00	b0.....
000000B0	04	00	00	00	00	00	01	00	10	04	00	00	F6	03	00	00	.....0.....c0.....
000000C0	00	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	.....0.....0.....
000000D0	14	04	00	00	06	04	00	00	00	00	00	00	00	00	00	00	0000000000
000000E0	04	00	00	00	00	00	01	00	10	04	00	00	00	04	00	00	0000000000
000000F0	00	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	0000000000
00000100	10	04	00	00	26	04	00	00	00	00	00	00	00	00	00	00	0000000000
00000110	04	00	00	00	00	00	01	00	10	04	00	00	36	04	00	00	0000000000
00000120	00	00	00	00	00	00	00	00	04	00	00	00	00	00	01	00	0000000000
00000130	10	04	00	00	46	04	00	00	00	00	00	00	00	00	00	00	0000000000
00000140	04	00	00	00	00	00	01	00	10	04	00	00	56	04	00	00	0000000000
00000150	00	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	0000000000
00000160	10	04	00	00	66	04	00	00	00	00	00	00	00	76	04	00	0000000000
00000170	04	00	00	00	00	00	01	00	10	04	00	00	76	04	00	00	0000000000
00000180	00	00	00	00	00	00	00	00	04	00	00	00	00	00	01	00	0000000000
00000190	01	00	00	00	98	01	00	80	00	00	00	00	00	00	00	00	0000000000
000001A0	04	00	00	00	00	00	00	00	10	04	00	00	86	04	00	00	0000000000
000001B0	04	00	00	00	00	00	00	00	04	00	00	00	01	00	00	00	0000000000
000001C0	00	00	00	00	80	00	00	00	00	00	00	00	00	00	00	00	0000000000
000001D0	0C	00	00	00	10	02	00	80	05	00	00	00	28	02	00	00	0000000000
000001E0	00	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	0000000000
000001F0	10	04	00	00	96	04	00	00	00	00	00	00	00	00	00	00	0000000000
00000200	04	00	00	00	00	00	01	00	10	04	00	00	A6	04	00	00	0000000000
00000210	00	00	00	00	00	00	00	00	04	00	00	00	00	00	01	00	0000000000
00000220	10	04	00	00	B6	04	00	00	00	00	00	00	00	00	00	00	0000000000
00000230	04	00	00	00	00	00	01	00	10	04	00	00	C6	04	00	00	0000000000
00000240	00	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	0000000000
00000250	03	00	00	00	70	02	00	80	02	00	00	00	88	02	00	00	0000000000
00000260	03	00	00	00	A0	02	00	80	18	00	00	00	B8	02	00	00	0000000000
00000270	00	00	00	00	00	00	00	00	04	00	00	00	00	00	01	00	0000000000
00000280	10	04	00	00	D6	04	00	00	00	00	00	00	00	00	00	00	0000000000
00000290	04	00	00	00	00	00	01	00	10	04	00	00	B6	04	00	00	0000000000
000002A0	00	00	00	00	00	00	00	00	04	00	00	00	00	00	00	01	0000000000
000002B0	10	04	00	00	F6	04	00	00	00	00	00	00	00	00	00	00	0000000000
000002C0	04	00	00	00	00	00	00	01	00	10	04	00	00	06	05	00	0000000000
000002D0	00	00	00	00	00	00	00	00	04	00	00	00	00	02	00	00	0000000000
000002E0	D2	03	00	80	F0	02	00	80	E2	03	00	80	08	03	00	80	0000000000

(le sezioni di cui si compone il malware è possibile trovarla sotto **sections headers**)

Si possono identificare cinque sezioni principali. Queste sezioni sono standard per i file **PE (Portable Executable)** di Windows e contengono diversi tipi di dati e codice.

1. **data:** Questa sezione contiene dati inizializzati e dati non inizializzati che il programma utilizza durante l'esecuzione. Include variabili globali o statiche che sono state inizializzate a un valore specifico nel codice sorgente. Significato in un Malware: I malware spesso usano .data per memorizzare stringhe critiche, URL di C2 (Command and Control), indirizzi IP codificati, chiavi crittografiche o configurazioni hardcoded che vengono lette all'avvio. Le caratteristiche (C0000040) indicano generalmente che la sezione è leggibile e scrivibile.
2. **rdata:** Descrizione: Questa sezione contiene dati di sola lettura (Read-only data). Include dati costanti, stringhe letterali (come i messaggi di errore), informazioni di debug o i metadati del file. Significato in un Malware: È spesso usata per memorizzare la Import Address Table (IAT), i nomi delle funzioni API importate, o stringhe costanti utilizzate dal malware. Le caratteristiche (40000040) indicano che la sezione è leggibile ma non scrivibile, rendendo i dati sicuri dalla modifica durante l'esecuzione.
3. **text:** Questa è la sezione più importante. Contiene il codice eseguibile effettivo (le istruzioni) del programma. Quando il sistema carica il file, l'esecuzione inizia tipicamente dal punto di ingresso (Entry Point) situato in questa sezione. Significato in un Malware: Contiene la logica operativa del malware: l'esecuzione delle API per iniettare codice, la crittografia dei file, la comunicazione di rete, ecc. Le caratteristiche (60000020) indicano che la sezione è leggibile ed eseguibile.
4. **idata:** Questa sezione contiene le risorse del programma, come icone, cursori, bitmap, menu, dialoghi, manifesti del programma (versioni) e stringhe di risorse non critiche. Significato in un Malware: I malware spesso usano la sezione .rsrc per nascondere dati binari importanti:  
Un payload iniettabile (come una DLL o un altro eseguibile) viene archiviato qui per essere estratto e iniettato in un altro processo.  
Chiavi crittografiche o altri dati di configurazione vengono nascosti tra i dati binari di risorse apparentemente innocue.  
L'hash dump mostrato nello screenshot in basso è proprio il contenuto della sezione .rsrc (Resource Directory), dove si notano blocchi di byte potenzialmente utili.
5. **rsrc:** Questa sezione contiene le informazioni necessarie per la rilocazione del codice e dei dati del programma. È usata quando il loader di Windows non può caricare il file all'indirizzo di memoria preferito specificato nell'intestazione PE e deve adattare gli indirizzi interni. Significato in un Malware: Il fatto che questa sezione sia presente indica che il file è un eseguibile standard. L'assenza di questa sezione in un PE non dinamico è spesso un indicatore di tecniche di anti-analisi o compattazione/packing, poiché un file con rilocazioni eliminate (strippate) è più difficile da analizzare.

### **Considerazioni finali:**

Il file in analisi presenta le caratteristiche di un malware di tipo Remote Access Trojan (RAT) o un info-stealer, grazie alla sua capacità di eseguire logica complessa (.text), manipolare i servizi e la persistenza (ADVAPI32, KERNEL32), e potenzialmente evadere i controlli di sicurezza (ntdll.dll).

### **Analisi dinamica:**

avviamo il "programma" e attiviamo anche procmon come strumento per l'analisi dinamica è possibile vedere una sfilza di dati.

cercando quindi filtrare solo i dati con “notepad” nel “process name” è possibile vedere come ci siano continue richieste di connessione tcp all’indirizzo IP 192.168.50.100 e una chiusura di thread

Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
15:47:...	notepad-classic...	5888	TCP Reconnect	DESKTOP-9K1O4BT.homenet.telecomit...	SUCCESS	Length: 0, seqnum:...
15:48:...	notepad-classic...	5888	TCP Reconnect	DESKTOP-9K1O4BT.homenet.telecomit...	SUCCESS	Length: 0, seqnum:...
15:48:...	notepad-classic...	5888	TCP Reconnect	DESKTOP-9K1O4BT.homenet.telecomit...	SUCCESS	Length: 0, seqnum:...
15:48:...	notepad-classic...	5888	Thread Exit		SUCCESS	Thread ID: 4500, ...
15:48:...	notepad-classic...	5888	Thread Exit		SUCCESS	Thread ID: 4696, ...
15:48:...	notepad-classic...	5888	TCP Reconnect	DESKTOP-9K1O4BT.homenet.telecomit...	SUCCESS	Length: 0, seqnum:...
15:48:...	notepad-classic...	5888	TCP Reconnect	DESKTOP-9K1O4BT.homenet.telecomit...	SUCCESS	Length: 0, seqnum:...

## Analisi con Cuckoo:

**Summary**

**File notepad-classico.exe**

Summary	<a href="#">Download</a>	<a href="#">Resubmit sample</a>
Size 282.5KB		
Type PE32 executable (GUI) Intel 80386, for MS Windows		
MD5 8a00a5c59ac157754ca575d721bcf900		
SHA1 c31e260630d653e2000f8e5f8dc270c751780d9		
SHA256 d2ec9f9273663f3218bc7dcbfb3b6f599fbce7a4ba986f9bbff77e3683988f2		
SHAS12 <a href="#">Show SHAS12</a>		
CRC32 97668313		
ssdeep None		
Yara	<ul style="list-style-type: none"> <li>CrowdStrike_CSIT_16018_03 - Metasploit payload loader</li> <li>DebuggerCheck__QueryInfo - (no description)</li> <li>anti_dbg - Checks if being debugged</li> <li>inject_thread - Code injection with CreateRemoteThread in a remote process</li> <li>network_http - Communications over HTTP</li> <li>network_dns - Communications use DNS</li> <li>network_dga - Communications using dga</li> <li>escalate_priv - Escalade privileges</li> <li>screenshot - Take screenshot</li> <li>win_mutex - Create or check mutex</li> </ul>	

**Score**  
This file is very suspicious, with a score of 10 out of 10!

**Feedback**  
Please notice: The scoring system is currently still in development and should be considered an alpha feature.

**Information on Execution**

**Analysis**

Category	Started	Completed	Duration	Routing	Logs
FILE	Nov. 18, 2025, 3:31 p.m.	Nov. 18, 2025, 3:40 p.m.	493 seconds	internet	<a href="#">Show Analyzer Log</a>
					<a href="#">Show Cuckoo Log</a>

**Signatures**

Yara rules detected for file (10 events)

description Metasploit payload loader	rule CrowdStrike_CSIT_16018_03
description (no description)	rule DebuggerCheck__QueryInfo
description Checks if being debugged	rule anti_dbg
description Code injection with CreateRemoteThread in a remote process	rule inject_thread
description Communications over HTTP	rule network_http
description Communications use DNS	rule network_dns
description Communication using dga	rule network_dga
description Escalade privileges	rule escalate_priv
description Take screenshot	rule screenshot
description Create or check mutex	rule win_mutex

File has been identified by 11 AntiVirus engines on IRMA as malicious (11 events)

File has been identified by 55 AntiVirus engines on VirusTotal as malicious (50 out of 55 events)