

ESERCIZIO W22D1

ANALISI DINAMICA BASICA

Mungiovì Fabio

TASK

Rispondere ai seguenti quesiti, con riferimento al file eseguibile **notepad-classico.exe** contenuto nel file zip:

<https://drive.google.com/file/d/1HNnJDSY7FbD1KHfiRzA2wVNHhzTJndUD/view?usp=sharing>

- Identificare eventuali azioni del malware sul file system utilizzando Process Monitor, fornendo una descrizione tramite AI;
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor, fornendo una descrizione tramite AI.

Suggerimento: ChatGPT (o altri LLM) possono ricevere in input degli screenshot da analizzare.

Facoltativo:

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

ESECUZIONE

Per l'esecuzione di questo esercizio è stato avviato, nel laboratorio di Malware Analysis, il malware **notepad-classico.exe**.

Tramite il tool Process Monitor sono stati filtrati i processi del malware (in immagine) e dati da analizzare al modello di AI Gemini.

15:07:43,3955578	notepad-classic...	9016	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input	SUCCESS	Desired Access: R...
15:07:43,3956092	notepad-classic...	9016	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Input	SUCCESS	KeySetInformation...
15:07:43,3956204	notepad-classic...	9016	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\ResyncResetTime	NAME NOT FOUND	Length: 16
15:07:43,3956312	notepad-classic...	9016	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\MaxResyncAttempts	NAME NOT FOUND	Length: 16
15:07:43,3956425	notepad-classic...	9016	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input	SUCCESS	
15:07:43,3997193	notepad-classic...	9016	CreateFile	C:\Windows\SystemResources\USER32.dll.mun	NAME NOT FOUND	Desired Access: R...
15:07:43,3998725	notepad-classic...	9016	CreateFile	C:\Windows\SystemResources\USER32.dll.mun	NAME NOT FOUND	Desired Access: R...
15:07:43,4090537	notepad-classic...	9016	RegOpenKey	HKCU	SUCCESS	Desired Access: R...
15:07:43,4090892	notepad-classic...	9016	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
15:07:43,4091312	notepad-classic...	9016	RegQueryKey	HKCU	SUCCESS	Query: Name
15:07:43,4091512	notepad-classic...	9016	RegOpenKey	HKCU\Software\Microsoft\CTF\DirectSwitchHotkeys	SUCCESS	Desired Access: R...
15:07:43,4091723	notepad-classic...	9016	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\CTF\DirectSwitchHotkeys	SUCCESS	KeySetInformation...
15:07:43,4091877	notepad-classic...	9016	RegCloseKey	HKCU	SUCCESS	
15:07:43,4092586	notepad-classic...	9016	RegEnumKey	HKCU\SOFTWARE\Microsoft\CTF\DirectSwitchHotkeys	NO MORE ENTRI...	Index: 0, Length: 2...
15:07:43,4092745	notepad-classic...	9016	RegCloseKey	HKCU\SOFTWARE\Microsoft\CTF\DirectSwitchHotkeys	SUCCESS	
15:07:44,3786786	notepad-classic...	9016	TCP Reconnect	DESKTOP-F0U2FJO-61733 -> 192.168.50.100:9001	SUCCESS	Length: 0, sequen:...
15:07:46,4102778	notepad-classic...	9016	TCP Reconnect	DESKTOP-F0U2FJO-61733 -> 192.168.50.100:9001	SUCCESS	Length: 0, sequen:...
15:07:50,4105696	notepad-classic...	9016	TCP Reconnect	DESKTOP-F0U2FJO-61733 -> 192.168.50.100:9001	SUCCESS	Length: 0, sequen:...
15:07:58,4100996	notepad-classic...	9016	TCP Reconnect	DESKTOP-F0U2FJO-61733 -> 192.168.50.100:9001	SUCCESS	Length: 0, sequen:...
15:08:04,4258605	notepad-classic...	9016	TCP Disconnect	DESKTOP-F0U2FJO-61733 -> 192.168.50.100:9001	SUCCESS	Length: 0, sequen:...
15:08:13,3481531	notepad-classic...	9016	Thread Create		SUCCESS	Thread ID: 8812
15:08:13,3485038	notepad-classic...	9016	Thread Create		SUCCESS	Thread ID: 232
15:08:15,4565834	notepad-classic...	9016	TCP Reconnect	DESKTOP-F0U2FJO-61733 -> 192.168.50.100:9001	SUCCESS	Length: 0, sequen:...
15:08:17,4568923	notepad-classic...	9016	TCP Reconnect	DESKTOP-F0U2FJO-61733 -> 192.168.50.100:9001	SUCCESS	Length: 0, sequen:...
15:08:21,4726955	notepad-classic...	9016	TCP Reconnect	DESKTOP-F0U2FJO-61733 -> 192.168.50.100:9001	SUCCESS	Length: 0, sequen:...
15:08:29,5037893	notepad-classic...	9016	TCP Reconnect	DESKTOP-F0U2FJO-61733 -> 192.168.50.100:9001	SUCCESS	Length: 0, sequen:...
15:08:35,5039927	notepad-classic...	9016	TCP Disconnect	DESKTOP-F0U2FJO-61733 -> 192.168.50.100:9001	SUCCESS	Length: 0, sequen:...
15:08:43,3166697	notepad-classic...	9016	Thread Exit		SUCCESS	Thread ID: 8504, ...
15:08:43,3166723	notepad-classic...	9016	Thread Exit		SUCCESS	Thread ID: 8956, ...
15:08:43,3167187	notepad-classic...	9016	Thread Exit		SUCCESS	Thread ID: 8972, ...
15:08:46,5352766	notepad-classic...	9016	TCP Reconnect	DESKTOP-F0U2FJO-61733 -> 192.168.50.100:9001	SUCCESS	Length: 0, sequen:...

Questi i risultati:

Analisi delle Azioni del Malware (basata sull'immagine):

1. Azioni sul File System (usando Process Monitor):

Dallo screenshot di Process Monitor, si possono osservare le seguenti azioni relative al file system eseguite da "notepad-classico.exe":

- **Accesso a file DLL:** Il processo tenta di accedere e creare il file C:\Windows\SystemResources\USER32.dll.mun. Questi tentativi hanno dato esito "NAME NOT FOUND", suggerendo che il file potrebbe non esistere o non essere accessibile con i permessi richiesti.
- **Creazione di file:** Viene tentata la creazione del file C:\Windows\SystemResources\USER32.dll.mun. Anche questo tentativo ha dato esito "NAME NOT FOUND".

2. Azioni su Processi e Thread (usando Process Monitor):

Dallo screenshot di Process Monitor, si possono osservare le seguenti azioni relative a processi e thread eseguite da "notepad-classico.exe":

- **Creazione di Thread:** Si notano diverse voci "Thread Create", che indicano la creazione di nuovi thread da parte del processo. Questo è un comportamento comune per le applicazioni legittime, ma nel contesto di un'analisi malware, potrebbe indicare l'avvio di nuove routine o funzionalità.
- **Uscita di Thread:** Sono presenti anche voci "Thread Exit", che indicano la terminazione dei thread precedentemente creati.
- **Connessioni di Rete (TCP Connect/Reconnect/Disconnect):** Il processo stabilisce connessioni TCP e riconnessioni a un indirizzo IP 192.168.50.100:9001. Successivamente, queste connessioni vengono disconnesse. Le connessioni di rete sono un indicatore significativo per il malware, suggerendo la comunicazione con un server remoto, che potrebbe essere per il controllo e comando (C2) o per l'esfiltrazione di dati.

Considerazione Finale sul Malware:

Basandosi sulle informazioni raccolte, "notepad-classico.exe" mostra comportamenti sospetti che vanno oltre la normale funzionalità di un'applicazione Notepad. In particolare:

- I tentativi di accesso e creazione di file di sistema (USER32.dll.mun) che falliscono potrebbero indicare un tentativo di persistenza o di iniezione di codice, anche se in questo caso non riuscito.
- La creazione e terminazione di thread sono attività normali, ma la loro combinazione con le connessioni di rete aumenta la sospetto.
- La presenza di connessioni TCP attive verso un indirizzo IP specifico (192.168.50.100:9001) è l'indicatore più forte di un potenziale comportamento dannoso. Questo suggerisce che il presunto "notepad-classico.exe" non è una semplice applicazione locale, ma un programma che tenta di comunicare con un host remoto. Questa comunicazione potrebbe servire per scaricare ulteriori payload, inviare informazioni dal sistema compromesso o ricevere comandi da un attaccante. Senza ulteriori analisi del traffico di rete e del payload scambiato, non è possibile determinare lo scopo esatto di questa comunicazione, ma è un chiaro segno di un potenziale malware.