

**Adrenaline RX (Anti-Ransomware / File-Monitor)**

**Versione Documento: 0.0.1.5**

**Versione Software: 3.5.0200.1**

## ***ADRENALINE RX GUIDA UTENTE***

### **Introduzione**

La proliferazione dei ransomware rappresenta una delle minacce più gravi per la sicurezza informatica contemporanea. I ransomware criptano i dati delle vittime, richiedendo un riscatto per la loro decriptazione. Le tradizionali misure di sicurezza, come antivirus e firewall, spesso non sono sufficienti a contrastare queste minacce in continua evoluzione.

*AdrenalineRX basa una combinazione di tecniche di analisi avanzata per rilevare e prevenire gli attacchi ransomware.*

### **Architettura e Funzionamento di AdrenalineRX**

AdrenalineRX esamina ogni file creato nel sistema come: entropia del file, entropia nel nome, byte magic, estensione del file, flusso IO dei file e gestione dei file canarino.

## Entropia del File

L'entropia di un file è una misura del disordine o della casualità nei dati contenuti nel file stesso. In generale, un file criptato presenta un'entropia significativamente più alta rispetto a un file non criptato. AdrenalineRX calcola l'entropia di ogni file per identificare potenziali attività di criptazione. Se l'entropia supera una soglia predefinita, il file viene contrassegnato come sospetto.

$$H(X) = - \sum_{i=1}^n P(x_i) \log_b P(x_i)$$

## Byte Magic

Il termine "byte magic" si riferisce alla presenza di sequenze di byte caratteristiche all'inizio dei file che identificano il tipo di file. Queste sequenze, note anche come "magic numbers", sono utilizzate da AdrenalineRX per verificare la coerenza tra il contenuto del file e la sua estensione dichiarata.

## Flusso IO dei File

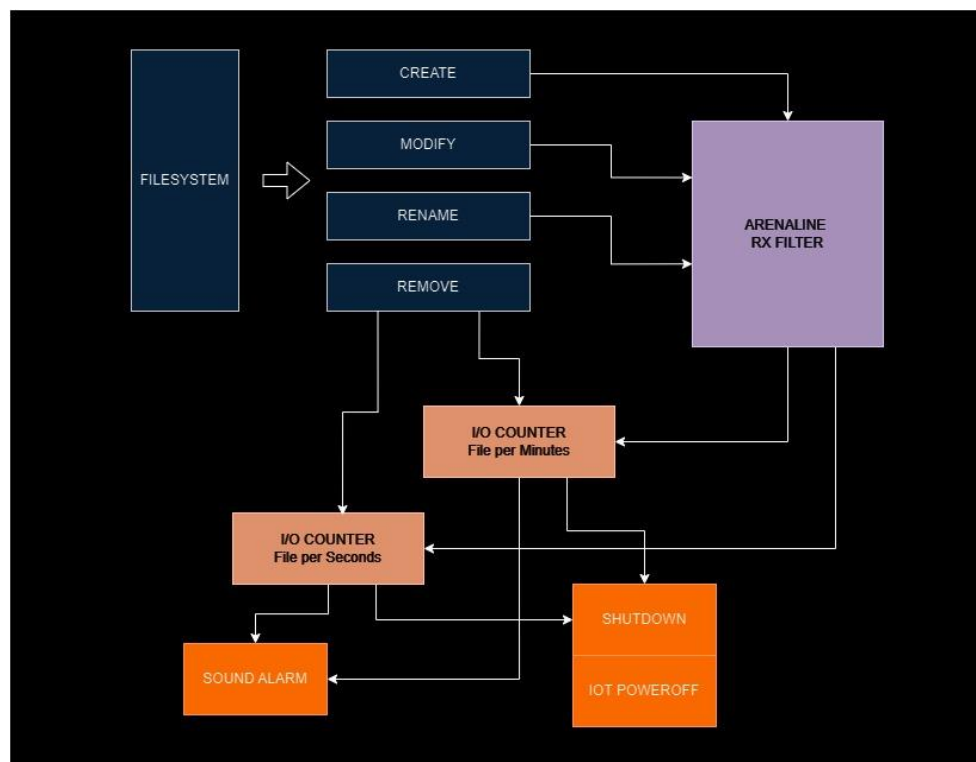
AdrenalineRX analizza in tempo reale le operazioni di input/output dei file nel filesystem, concentrandosi sulle operazioni di creazione, modifica, rinomina ed eliminazione. Un aumento anomalo in queste attività può essere indicativo di un ransomware che sta criptando file.

## File Canarino

AdrenalineRX utilizza anche file canarino come metodo di rilevamento. I file canarino sono file appositamente creati e monitorati che non dovrebbero mai essere modificati durante il normale utilizzo del sistema. Qualsiasi tentativo di accesso, modifica o eliminazione di questi file attiva immediatamente un allarme.

## Sinergia delle Tecniche di Rilevamento

La forza di AdrenalineRX risiede nella combinazione sinergica di questi parametri. Ogni tecnica fornisce un pezzo del puzzle, e insieme formano un sistema di rilevamento altamente efficace. L'approccio multi-parametrico permette di ridurre i falsi positivi e aumentare la precisione del rilevamento. AdrenalineRX non solo identifica i file sospetti, ma anche il comportamento complessivo del sistema, permettendo una risposta tempestiva e mirata alle minacce.



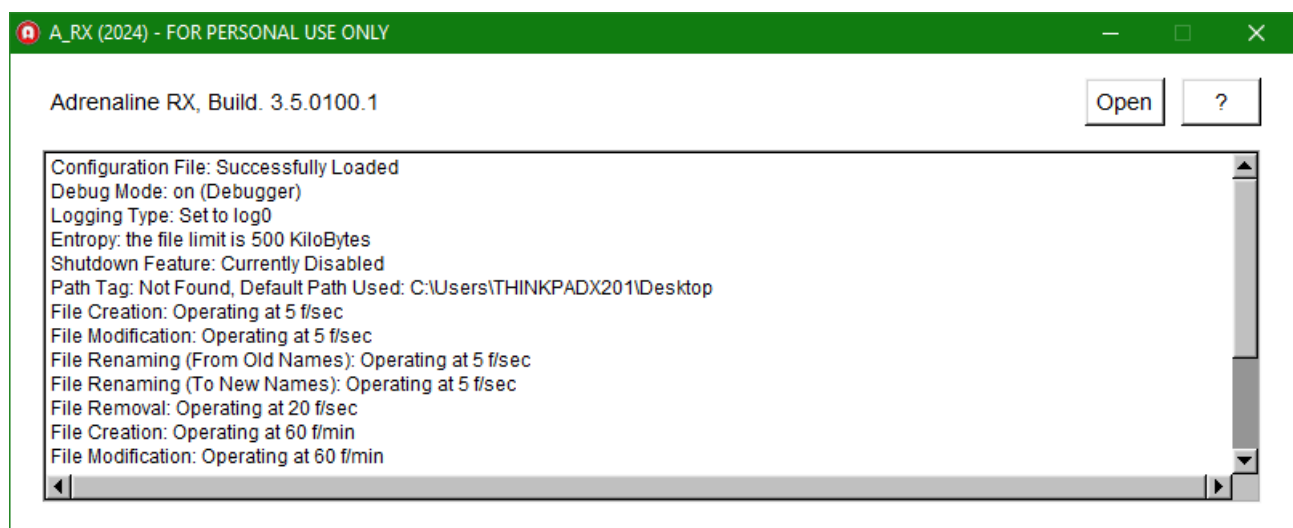
## Azioni di Contenimento Estremo

AdrenalineRX è progettato come ultima linea di difesa contro gli attacchi ransomware. Nel caso in cui un attacco riesca a superare le misure di rilevamento iniziali e inizi a criptare i file, AdrenalineRX è in grado di eseguire azioni di contenimento estremo. Tra queste, la più drastica è lo spegnimento immediato del sistema. Spegnere il sistema può interrompere il processo di criptazione, riducendo i danni ai file non ancora compromessi.

*Questa funzione è particolarmente utile quando tutte le altre misure di difesa sono fallite.*

## Avvio

Dopo essere stato avviato, AdrenalineRX visualizza una serie di dati iniziali per comprendere lo stato del programma e la sua configurazione attuale. Questi dati forniscono informazioni dettagliate sulle impostazioni e le funzionalità attive, tra cui il tipo di log utilizzato, lo stato della funzione di spegnimento, il percorso di monitoraggio dei file e le impostazioni di allarme per le operazioni di creazione, modifica, rinominazione e rimozione dei file.



## **Allarme Sonoro**

Quando AdrenalineRX rileva un'attività sospetta o potenzialmente dannosa, attiva un allarme sonoro per avvisare prontamente l'utente dell'attività anomala in corso. L'allarme sonoro è progettato per catturare immediatamente l'attenzione dell'utente e segnalare la presenza di un potenziale rischio per la sicurezza del sistema e viene utilizzato prelaventemente per attività di fine-tuning.

Il file "ALARM.wav", presente nella cartella radice di AdrenalineRX, contiene il suono dell'allarme utilizzato per questo scopo specifico. Questo file audio è progettato per essere facilmente riconoscibile e distintivo, garantendo che l'utente possa identificare rapidamente l'avviso di una potenziale minaccia.

Gli allarmi sonori svolgono un ruolo fondamentale nelle fasi di analisi e di test prima che AdrenalineRX entri in produzione effettiva. Durante questa fase, gli sviluppatori e gli analisti di sicurezza utilizzano gli allarmi sonori per verificare l'efficacia del sistema nel rilevare e segnalare attività sospette. Questo processo consente di valutare l'affidabilità del sistema e di apportare eventuali ottimizzazioni o miglioramenti necessari prima che AdrenalineRX venga distribuito in un ambiente di produzione.

## **Shut Down Automatico**

Quando AdrenalineRX individua un'attività dannosa, può avviare automaticamente la funzione di spegnimento del sistema per prevenire ulteriori danni e salvaguardare l'integrità dei dati. Questa funzionalità di spegnimento automatico è progettata per intervenire prontamente in situazioni critiche, proteggendo il sistema e i dati dall'espansione dei danni causati da attività malevole.

## File di Configurazione dei Magic Bytes (magic.cfg)

Nel file di configurazione, ogni riga specifica un tipo di file con la relativa estensione e il corrispondente "Magic Byte" utilizzato per identificare il tipo di file. I magic bytes sono sequenze di byte uniche che si trovano all'inizio di un file e sono utilizzate per determinare il suo tipo o formato. Questi valori vengono poi utilizzati da Adrenaline per riconoscere e gestire correttamente i diversi tipi di file durante le analisi e le operazioni di protezione.



```
File  Modifica  Formato  Visualizza  ?
.zip 50 48
.rar 52 61 72 21
.crdownload 52 61 72 21
.7z 37 7A
.crdownload 7z 37 7A
.webp 52 49 46 46
.pdf 25 50 44 46
.crdownload 25 50 44 46
.png 89 50 4E 47
.crdownload 89 50 4E 47
.m3u8 23 45 58 54 4D 33 55
.m3u 23 45 58 54 4D 33 55
.iso 43 44 30 30 31
.cdi 43 44 30 30 31
.jpeg FF D8 FF
.gif 47 49 46 38
.bmp 42 4D
.mpg 47
.mpg 00 00 01 BA
.mpeg 00 00 01 BA
.vob 00 00 01 BA
.m2p 00 00 01 BA
.mpg 00 00 01 B3
.mpeg 00 00 01 B3
.mov 6D 6F 6F 76
.m4v 3F 53 4D 4C
```

## Installazione

Per configurare Adrenaline Rx, segui attentamente questi passaggi:

- 1- **Avvia Adrenaline Rx:** Dopo aver installato il programma, avvialo facendo doppio clic sull'icona dell'applicazione.
- 2- **Configurazione iniziale:** Adrenaline Rx si aprirà con i valori di default. Inizierà a monitorare la directory predefinita, di solito C:/Users/utente/Desktop.
- 3- **Apri il file di configurazione:** Per personalizzare le impostazioni, premi il pulsante "Open" dall'interfaccia di Adrenaline Rx. Questo ti permetterà di accedere al file di configurazione, di solito chiamato config.cfg.
- 4- **Modifica le impostazioni:** Utilizzando un editor di testo, apri il file config.cfg e modifica le impostazioni secondo le tue esigenze. Puoi specificare i percorsi da monitorare, regolare le impostazioni di rilevamento e altro ancora.
- 5- **Salva e chiudi:** Una volta apportate le modifiche, salva il file config.cfg e chiudi l'editor di testo.
- 6- **Riavvia Adrenaline Rx:** Per applicare le modifiche, chiudi e riavvia Adrenaline Rx. In questo modo, il programma utilizzerà le nuove impostazioni configurate nel file config.cfg.

Seguendo questi passaggi, potrai personalizzare le impostazioni di Adrenaline Rx e configurare il programma per adattarlo alle tue esigenze specifiche di sicurezza informatica.

## File di Configurazione (config.cfg)

Il file di configurazione di Adrenaline (config.cfg) contiene le impostazioni principali del programma, come il tipo di log, lo stato della funzione di shutdown, il percorso di monitoraggio e le soglie per l'allarme sui file.

### File config.cfg :

```
7  IO_MONITOR=on
8
9  # LOG: Defines the logging level. Possible values are log0, log1, log2.
10 LOG=log1
11
12 # ENTROPY VALUE
13 ENTROPY=7.2
14
15 # FILE_LIMITER: Limits the entropy frame.
16 # The value represents the KiloBytes to scan.
17 FILE_LIMITER=500
18
19 # CANARY_HIDE: Enables or disables la creazione di Canary Files with Hide Attribute. Possible values are 'on' and 'off'.
20 CANARY_HIDE=off
21
22 # MAX_CANARY_ALARM: indica il massimo numero dei canarini che generano un allarme
23 MAX_CANARY_ALARM=2
24
25 # POWER: Enables or disables the shutdown function. Possible values are 'on' and 'off'.
26 # Use on in production.
27 CAUTION!! Use POWER=on with CAUTELE!
28 POWER=off
29
30 # PATH: Sets the path to monitor (recursive).
31 # If the path is not found, Adrenaline uses the default path: c:\Users\<User>\Desktop.
32 # If the path is entire <drive> (C,D,E,F,G) do not use backslash, example C:\ use C: without backslash
33 PATH=C:
34
35 # CREATE, MODIFY, RENAME_OLD, RENAME_NEW, REMOVE:
36 # Set the number of file operations per second that will trigger the alarm.
37 # When set to 0, the IO Filter is disabled.
38 CREATE=5
39 MODIFY=5
40 RENAME_OLD=5
41 RENAME_NEW=5
42 REMOVE=0
43
44 # CREATE_M, MODIFY_M, RENAME_OLD_M, RENAME_NEW_M, REMOVE_M:
45 # Set the number of file operations per minute that will trigger the alarm.
46 # When set to 0, the IO Filter is disabled.
47 CREATE_M=200
48 MODIFY_M=200
49 RENAME_OLD_M=200
50 RENAME_NEW_M=200
51 REMOVE_M=0
52
53 # CLOSE_BUTTON: Defines the behavior of the "X" window button.
54 # When set to 'off', the window can be closed using the "X" button.
```

**Nota:** è importante notare che i comandi sono sensibili alle maiuscole/minuscole, quindi assicurati di rispettare correttamente la sintassi durante la modifica del file di configurazione.

Elenco dei comandi che puoi configurare all'interno del file config.cfg::



**Command:** LOG=<log0 | log1> Il file di log,

**Used for:** Fine-tuning / File Tracking

Essenziale per il tracciamento delle attività e per l'ottimizzazione delle prestazioni, viene generato quotidianamente e può essere trovato nella directory principale di Adrenaline, specificamente nella cartella ".\log".

**log0:** Questa modalità di registrazione è inattiva, non registrando alcun evento.

**log1:** Abilita questa modalità per visualizzare i file processati da AdrenalineRX. Questa modalità è particolarmente utile per capire il "rumore" generato dalla lettura del filesystem. Se noti che ci sono file o cartelle che vengono letti ma che non dovrebbero essere inclusi nel processo, puoi aggiustare le tue impostazioni di esclusione per ignorare questi file o cartelle in futuro. In questo modo, i log ti aiutano a ottimizzare le prestazioni di AdrenalineRX, riducendo il tempo speso a leggere file o cartelle non necessari e migliorando l'efficienza del tuo processo. Ricorda, tuttavia, che ogni modifica alle impostazioni di esclusione dovrebbe essere fatta con attenzione, per evitare di escludere accidentalmente file o cartelle importanti.

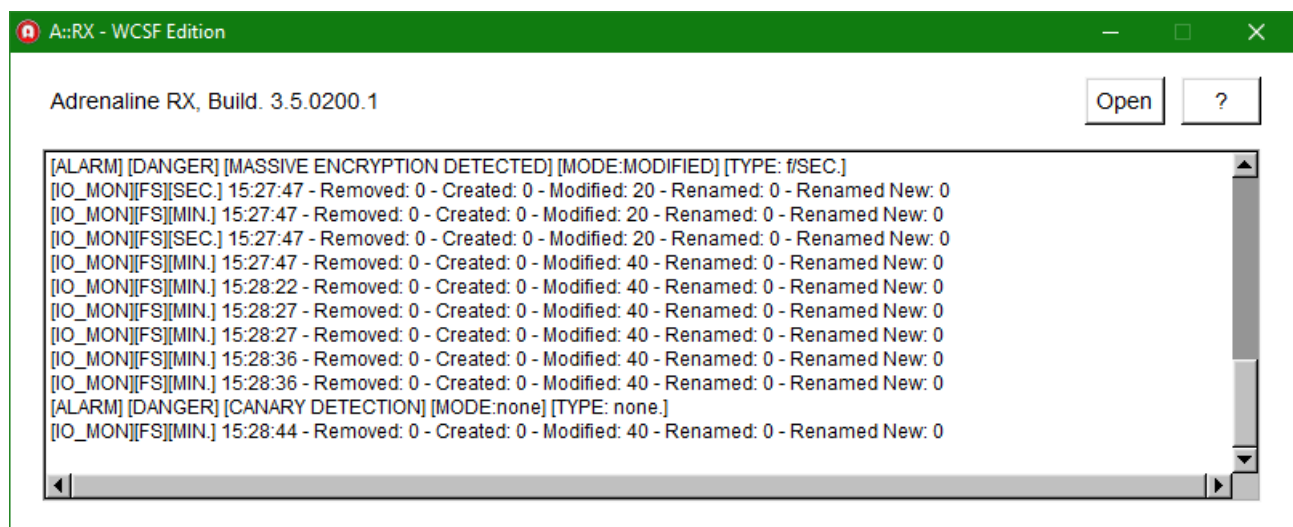
**Command:** IO\_MONITOR=<on|off>

**Used for:** Fine-tuning

Questa modalità consente di visualizzare il numero dei file al secondo e al minuto, fornendo informazioni utili per regolare correttamente i valori di soglia nei trigger di allarme.

La modalità IO\_MONITOR si disattiva automaticamente dopo 100 rilevamenti, garantendo che non venga utilizzata eccessivamente.

L'utilizzo della modalità IO\_MONITOR è prezioso perché consente agli utenti di comprendere meglio le attività del filesystem e di regolare accuratamente i parametri dei trigger di allarme per adattarli alle loro esigenze specifiche di sicurezza.



In questo esempio (immagine sopra)

-Il contatore "Removed" tiene traccia di tutti i file eliminati, mentre gli altri parametri vengono filtrati attraverso gli algoritmi di Adrenaline RX.

-I file che i filtri di Adrenaline RX ha reputato puliti non risulteranno nei contatori.

**Command:** POWER=<on|off>

**Used for:** Ultima Difesa

Il comando POWER attiva o disattiva la funzione di spegnimento del computer in risposta a un allarme critico rilevato dall'antiransomware. Quando questa funzione è attivata, il sistema si spegnerà automaticamente dopo che l'antiransomware ha rilevato un'allerta critica, come un tentativo di crittografia di massa da parte di un ransomware.

Questo meccanismo di spegnimento automatico è progettato per limitare i danni in caso di attacco ransomware. Quando viene rilevata un'attività sospetta o dannosa che potrebbe compromettere la sicurezza dei dati, l'antiransomware attiva l'allarme critico e, se la funzione di spegnimento automatico è abilitata, il computer si spegne immediatamente per impedire ulteriori danni.

Questo è un importante strumento di difesa per proteggere i dati sensibili e prevenire la diffusione del ransomware nel sistema, consentendo agli utenti di rispondere prontamente e limitare l'impatto degli attacchi informatici. Tuttavia, è importante utilizzare questa funzione con cautela, poiché lo spegnimento del computer interrompe tutte le attività in corso.

**TIPS:** *Abilita il comando "POWER=on" solo quando sei sicuro di aver configurato il file exclude.cfg*

**Command:** PATH=<path>

**Used for:** lettura filesystem

Questo comando specifica il percorso in cui il monitor inizia la scansione in modalità ricorsiva, controllando tutte le sottodirectory all'interno del percorso specificato.

Se il percorso PATH non è definito correttamente AdrenalineRX usa il percorso predefinito è C:\Users\utente\Desktop\

È possibile utilizzare anche lettere di unità come C:, ma questo genera molto rumore. Per ridurre il rumore, è necessario configurare il file exclude.cfg aggiungendo i percorsi rumorosi da escludere dal monitoraggio.

**Command:** FILE\_LIMITER=<KiloBytes>

**Used for:** Entropy Limiter

Questo comando determina la dimensione del primo segmento di dati, o “frame”, che il motore entropico analizza.

**Command:** CREATE=<file per second>

CREATE\_M=<file per minute>

MODIFY=<file per second>

MODIFY\_M=<file per minute>

RENAME\_OLD=<file per second>

RENAME\_OLD\_M=<file per minute>

RENAME\_NEW=<file per second>

RENAME\_NEW\_M=<file per minute>

Questi comandi consentono di impostare il trigger per gli allarmi legati al filesystem, espressi in secondi/minuto. Quando viene specificato un valore, Adrenaline RX monitora il numero di file creati nel sistema ogni secondo/minuto.

Se il numero di file supera il valore specificato, viene attivato un allarme.

Se viene impostato il valore di zero ( es. CREATE=0, allora il parametro non viene valutato).

Ad esempio, se imposti CREATE=4 nel file config.cfg e vengono creati 5 file in un secondo, Adrenaline RX rivaluterà lo score del filtro interno per segnalare un'elevata attività di creazione dei file.

**Command:** REMOVE=<file per second>

REMOVE\_M=<file per minute>

Questi comandi impostano il trigger per gli allarmi di rimozione dei file, espressi rispettivamente in secondi e in minuti. Quando viene specificato un valore, Adrenaline RX monitora il numero di file rimossi dal sistema nel periodo di tempo corrispondente. Se il tempo trascorso dalla rimozione di un file supera il valore specificato, viene attivato un allarme.

Tuttavia, è fondamentale valutare attentamente l'utilizzo di questi comandi quando si configurano i percorsi di monitoraggio, specialmente se si stanno monitorando percorsi del sistema operativo o altre directory ad alto rumore. Ad esempio, se si stanno monitorando i file di sistema del sistema operativo, potrebbero verificarsi frequenti rimozioni di file che non sono necessariamente indicative di un attacco o di un comportamento sospetto. In questi casi, l'attivazione degli allarmi basati sul tempo potrebbe generare falsi positivi e creare confusione.

Pertanto, è consigliabile valutare attentamente la configurazione dei trigger di rimozione dei file, tenendo conto del contesto operativo e delle caratteristiche specifiche del sistema. È possibile ridurre il rischio di falsi positivi regolando i valori

dei trigger in base alla frequenza attesa di rimozione dei file nel contesto specifico del monitoraggio. Questo permette di mantenere un equilibrio tra la sensibilità del sistema di allarme e la riduzione dei falsi positivi, garantendo che gli avvisi siano genuini e rilevanti per la sicurezza del sistema.

Per ottimizzare la configurazione dei trigger di rimozione dei file, è consigliabile utilizzare la modalità IO\_MONITOR per monitorare attentamente l'attività del sistema. Questo permette di valutare con precisione la frequenza delle rimozioni dei file e di calibrare i trigger nel file config.cfg in modo appropriato. L'utilizzo della modalità IO\_MONITOR consente di adattare i trigger in base al contesto operativo e alle caratteristiche specifiche del sistema, riducendo al minimo il rischio di falsi positivi e garantendo che gli avvisi siano genuini e rilevanti per la sicurezza del sistema.

**Command:** MAX\_CANARY\_ALARM=<file\_per\_session>

Il comando MAX\_CANARY\_ALARM consente di specificare il numero massimo di file Canarino che possono essere erroneamente manipolati dall'utente prima che venga attivato un allarme. Questa impostazione definisce una soglia di errore per il sistema di allarme rispetto ai file Canarino e conta per tutta la durata della sessione di Adrenaline RX, indipendentemente dai filtri attivi.

Ad esempio, se si imposta MAX\_CANARY\_ALARM=2, significa che devono essere manipolati almeno due file Canarino durante l'intera sessione di utilizzo di Adrenaline RX prima che venga attivato un allarme.

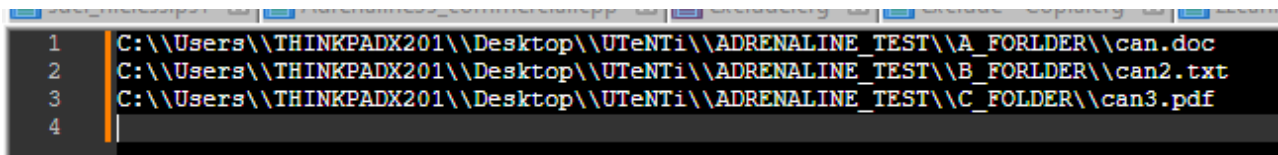
**Command:** CANARY\_HIDE=<on | off>

Valore consigliato: off

Quando il flag CANARY\_HIDE è impostato su "on" e i file Canarino vengono generati con l'attributo "nascosto", non saranno visibili all'interno di Esplora file (File Explorer) in Windows, a meno che l'utente non abbia attivato l'opzione "Mostra tutti i file nascosti".

## File canary.cfg :

Contiene i percorsi e il nome dei file che vengono generati da Adrenaline RX:



```
1 C:\\Users\\THINKPADX201\\Desktop\\UTeNTi\\ADRENALINE_TEST\\A_FORLDER\\can.doc
2 C:\\Users\\THINKPADX201\\Desktop\\UTeNTi\\ADRENALINE_TEST\\B_FORLDER\\can2.txt
3 C:\\Users\\THINKPADX201\\Desktop\\UTeNTi\\ADRENALINE_TEST\\C_FOLDER\\can3.pdf
4
```

## Command: ENTROPY=<float>

Il comando ENTROPY nel file di configurazione di Adrenaline RX consente di regolare il parametro dell'entropia minima. Questo parametro definisce la soglia minima di entropia che un file deve avere affinché venga considerato come potenzialmente sospetto o dannoso.

## Escludere i percorsi:

Una delle funzionalità di Adrenaline RX è la possibilità di escludere determinati percorsi di file dalle scansioni, per evitare falsi positivi o per migliorare le prestazioni durante l'analisi.

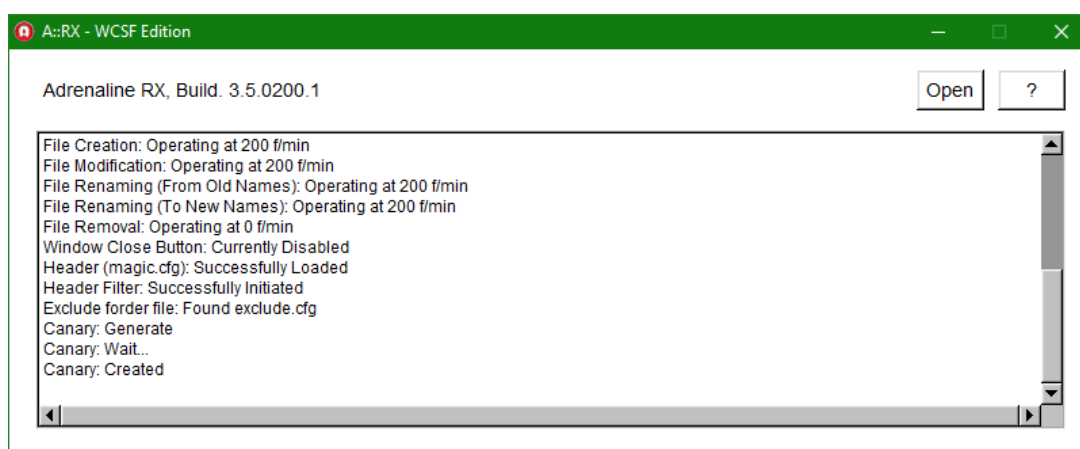
Questo è particolarmente utile per percorsi che contengono file di sistema o dati di applicazioni che non richiedono monitoraggio.

Per configurare le esclusioni dei percorsi in AdrenalineRX, è necessario editare il file **exclude.cfg**, situato nella directory di configurazione del programma. Seguire questi passaggi per escludere i percorsi desiderati:

```
1 C:\\\\Windows\\
2 C:\\\\Program Files\\
3 C:\\\\ProgramData\\
4 C:\\\\Users\\THINKPADX201\\AppData\\
5
```

## 1- Individuare il File config.cfg, exclude.cfg, canary.cfg , magic.cfg e Log.

- Il file di configurazione si trovano tipicamente nella cartella di installazione di AdrenalineRX. Premi il bottone “Open” per raggiungere la cartella di installazione.



## 2- Aprire il File per la Modifica:

- Utilizzare un editor di testo come Notepad o Notepad++ o qualsiasi altro editor di testo preferito per aprire exclude.cfg.

**TIPS: Abilitando LOG=log1**, è possibile monitorare il rumore generato dalle cartelle che non sono state escluse dal monitoraggio. Questo permette di identificare e aggiungere le cartelle rumorose al file exclude.cfg



## Schema di Versionamento

Il sistema di versionamento di Adrenaline Rx segue uno schema standard composto da quattro numeri:

- Versione principale: Indica una versione significativa del software con importanti modifiche o aggiunte di funzionalità.
- Revisione maggiore: Rappresenta una revisione più piccola rispetto alla versione principale, generalmente caratterizzata da miglioramenti significativi o aggiornamenti importanti.
- Revisione minore: Indica una revisione più piccola rispetto alla revisione maggiore, che include aggiustamenti minori, correzioni di bug o miglioramenti di prestazioni.
- Numero di bug: Rappresenta il numero di bug corretti dalla versione.

Ad esempio, consideriamo la versione "3.5.0100.0":

- "3" è la versione principale.
- "5" è la revisione maggiore.
- "0100" è la revisione minore.
- "0" indica il numero di bug corretti.