

Adrenaline RX (Anti-Ransomware / File-Monitor)

Versione Documento: 0.0.1.3

Versione Software: 3.5.0100.1

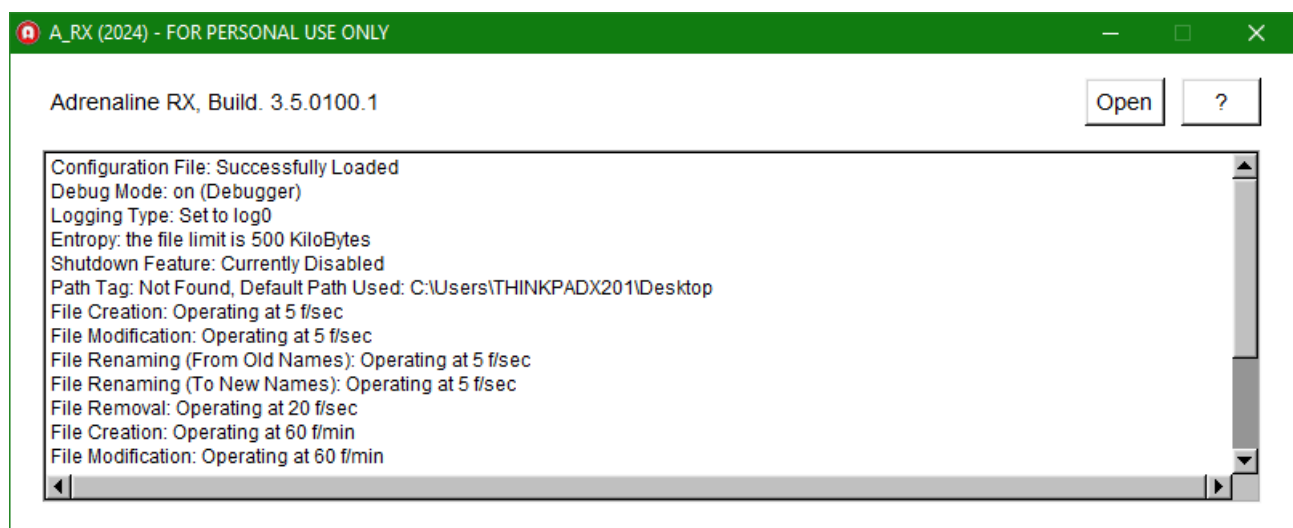
Author: Roberto Mazzoni, Federico Bombardi

Introduzione

Adrenaline RX è un antiransomware scritto in C++ progettato per proteggere i tuoi dati sensibili e impedire l'accesso non autorizzato ai tuoi file. Con una combinazione di tecniche avanzate di monitoraggio e rilevamento, Adrenaline RX offre una difesa robusta contro minacce informatiche come il ransomware. Grazie alle sue funzionalità di calcolo dell'entropia, allarme sonoro e shutdown automatico, Adrenaline è uno strumento indispensabile per mantenere al sicuro i tuoi dati da attacchi ransomware quando le normali difese sono cadute o addirittura non esistono o sono troppo deboli per bloccare l'attacco in atto.

Log Iniziale

Durante l'avvio, Adrenaline visualizza un log iniziale per fornire informazioni sullo stato del programma e della configurazione corrente. Questo log include dettagli come il tipo di log, lo stato della funzione di shutdown, il percorso di monitoraggio e le impostazioni di allarme per creazione, modifica, rinominazione e rimozione dei file.



Funzionalità Principali

I filtri di Adrenaline RX generano il punteggio in base al calcolo dell'Entropia, Intestazioni, Estensioni e flussi I/O per la valutazione dei file generati e compromessi. Questo permette di identificare rapidamente i file che sono stati crittografati o modificati in modo anomalo.

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

Allarme Sonoro

Quando viene rilevata un'attività sospetta o potenzialmente dannosa, Adrenaline attiva un allarme sonoro per avvisare l'utente dell'attività sospetta in corso. Puoi trovare il file "ALARM.wav" nella cartella radice di Adrenaline.

Shutdown Automatico

In caso di rilevamento di un malware o di attività dannose, Adrenaline può attivare automaticamente la funzione di shutdown del sistema per impedire ulteriori danni e proteggere l'integrità dei dati.

File di Configurazione dei Magic Bytes (magic.cfg)

Il file di configurazione dei magic bytes di Adrenaline (magic.cfg) contiene le estensioni dei file e i corrispondenti "Magic Byte" per identificare il tipo di file.

.zip 50 4B

.rar 52 61 72 21

.....

Installazione

Per installare Adrenaline Rx, segui questi passaggi:

- Scarica il file di installazione dalla pagina ufficiale del progetto su GitHub.
- Esegui il file di installazione e segui le istruzioni visualizzate sullo schermo.
- Configura il file di config.cfg secondo le tue esigenze.
- Una volta completata l'installazione, avvia Adrenaline Rx.

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.

Attenzione: si noti che i caratteri dei comandi sono sensibili alle maiuscole/minuscole, quindi assicurati di rispettare correttamente la sintassi.

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

Command: LOG=<log0 | log1 | log2 >

Il file di log, essenziale per il tracciamento delle attività, 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:** In questa modalità, vengono registrati solo i file sospetti, quelli che potrebbero essere stati criptati. Il registro segue un formato standardizzato, mostrando la data, l'ora e il percorso del file.
- **log2: "Modalità monitor",** Questa modalità registra tutti gli eventi di creazione e manipolazione dei file, senza eccezioni. Ogni attività viene annotata nel file di log.

Command: DEBUG_MODE=<on|off>

Attiva la modalità debug.

!IMPORTANTE!: usare DEBUG MODE=off in produzione.

Command: POWER=<on|off>

Questo comando attiva o disattiva la funzione di shutdown del computer in risposta a un allarme critico rilevato dall'antiransomware.

Command: PATH=<path>

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

Command: FILE_LIMITER=<KiloBytes>

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

Command: CREATE=<file per second>

Imposta il trigger per gli allarmi di creazione dei file, espressi in secondi. Se il tempo di creazione di un file supera il valore specificato, l'allarme viene attivato.

Command: CREATE_M=<file per minute>

Imposta il trigger per gli allarmi di creazione dei file, espressi in secondi. Se il tempo di creazione di un file supera il valore specificato, l'allarme viene attivato.

Command: MODIFY=<file per second>

Imposta il trigger per gli allarmi di modifica dei file, espressi in secondi. Se il tempo trascorso dall'ultima modifica di un file supera il valore specificato, l'allarme viene attivato.

Command: MODIFY_M=<file per minute>

Imposta il trigger per gli allarmi di modifica dei file, espressi in secondi. Se il tempo trascorso dall'ultima modifica di un file supera il valore specificato, l'allarme viene attivato.

Command: RENAME_OLD=<file per second>

Imposta il trigger per gli allarmi di rinomina (vecchio nome), espressi in secondi. Se il tempo trascorso dall'ultima modifica del nome originale di un file supera il valore specificato, l'allarme viene attivato.

Command: RENAME_OLD_M=<file per minute>

Imposta il trigger per gli allarmi di rinomina (vecchio nome), espressi in secondi. Se il tempo trascorso dall'ultima modifica del nome originale di un file supera il valore specificato, l'allarme viene attivato.

Command: RENAME_NEW=<file per second>

Imposta il trigger per gli allarmi di rinomina (nuovo nome), espressi in secondi.

Command: RENAME_NEW_M=<file per minute>

Imposta il trigger per gli allarmi di rinomina (nuovo nome), espressi in secondi.

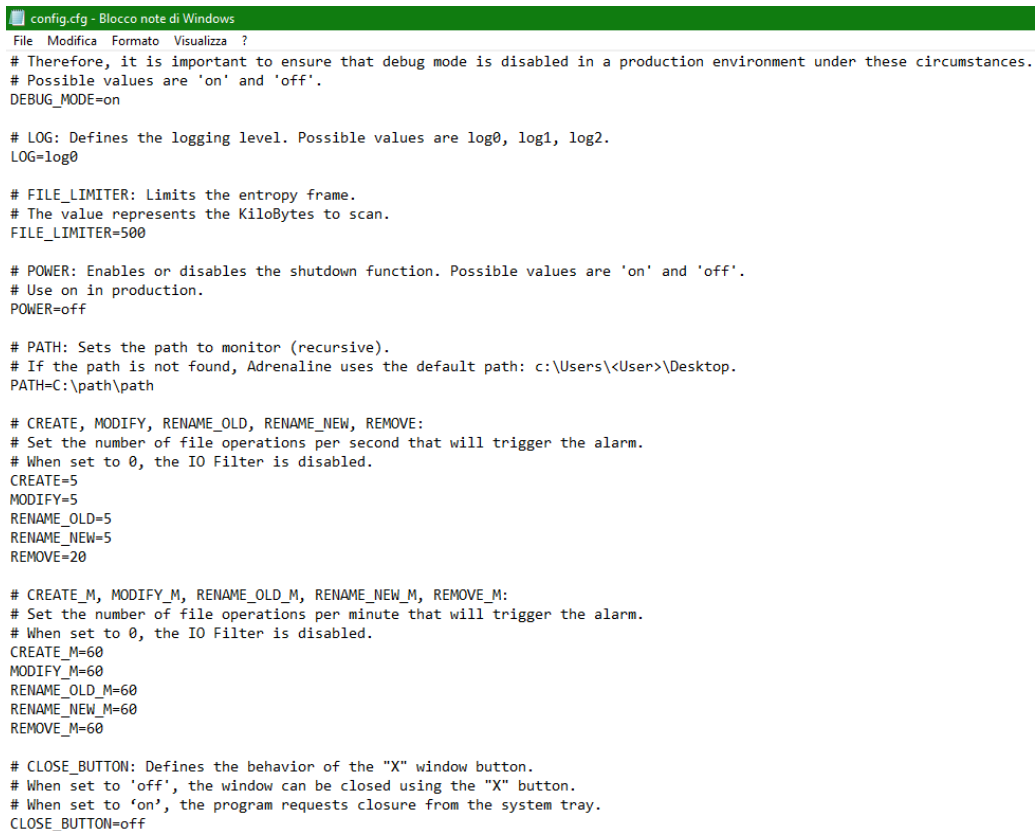
Command: REMOVE=<file per second>

Imposta il trigger per gli allarmi di rimozione dei file, espressi in secondi. Se il tempo trascorso dalla rimozione di un file supera il valore specificato, l'allarme viene attivato.

Command: REMOVE_M=<file per minute>

Imposta il trigger per gli allarmi di rimozione dei file, espressi in secondi. Se il tempo trascorso dalla rimozione di un file supera il valore specificato, l'allarme viene attivato.

config.cfg



```
config.cfg - Blocco note di Windows
File Modifica Formato Visualizza ?
# Therefore, it is important to ensure that debug mode is disabled in a production environment under these circumstances.
# Possible values are 'on' and 'off'.
DEBUG_MODE=on

# LOG: Defines the logging level. Possible values are log0, log1, log2.
LOG=log0

# FILE_LIMITER: Limits the entropy frame.
# The value represents the KiloBytes to scan.
FILE_LIMITER=500

# POWER: Enables or disables the shutdown function. Possible values are 'on' and 'off'.
# Use on in production.
POWER=off

# PATH: Sets the path to monitor (recursive).
# If the path is not found, Adrenaline uses the default path: c:\Users\<User>\Desktop.
PATH=C:\path\path

# CREATE, MODIFY, RENAME_OLD, RENAME_NEW, REMOVE:
# Set the number of file operations per second that will trigger the alarm.
# When set to 0, the IO Filter is disabled.
CREATE=5
MODIFY=5
RENAME_OLD=5
RENAME_NEW=5
REMOVE=20

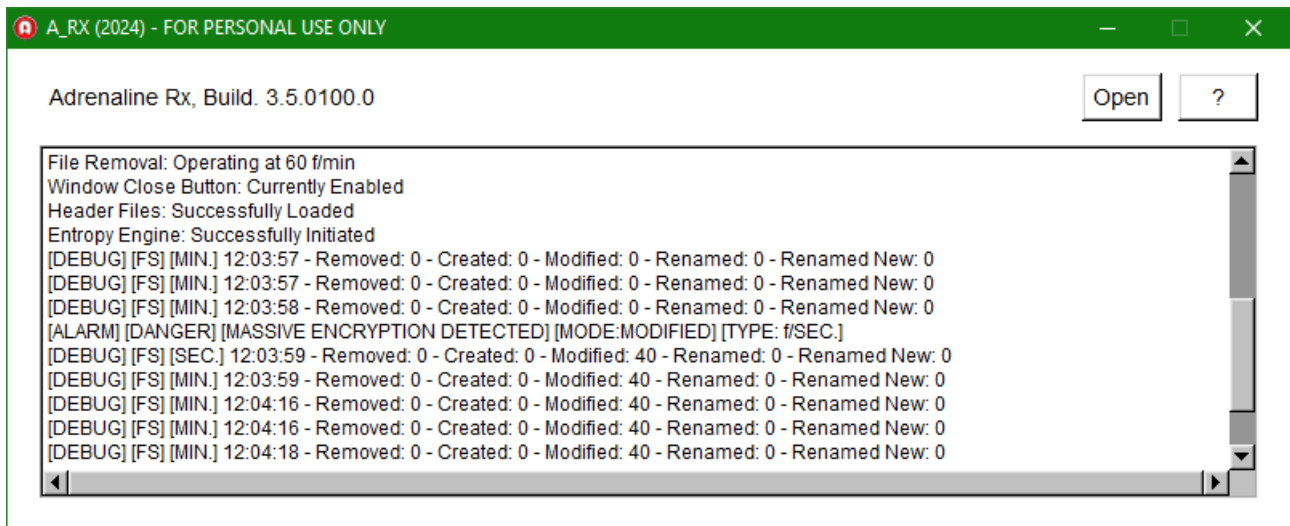
# CREATE_M, MODIFY_M, RENAME_OLD_M, RENAME_NEW_M, REMOVE_M:
# Set the number of file operations per minute that will trigger the alarm.
# When set to 0, the IO Filter is disabled.
CREATE_M=60
MODIFY_M=60
RENAME_OLD_M=60
RENAME_NEW_M=60
REMOVE_M=60

# CLOSE_BUTTON: Defines the behavior of the "X" window button.
# When set to 'off', the window can be closed using the "X" button.
# When set to 'on', the program requests closure from the system tray.
CLOSE_BUTTON=off
```

Debug Mode:

ATTENZIONE!, non usare la modalità Debug in produzione. Puoi disabilitare la modalità DEBUG nel file config.cfg.

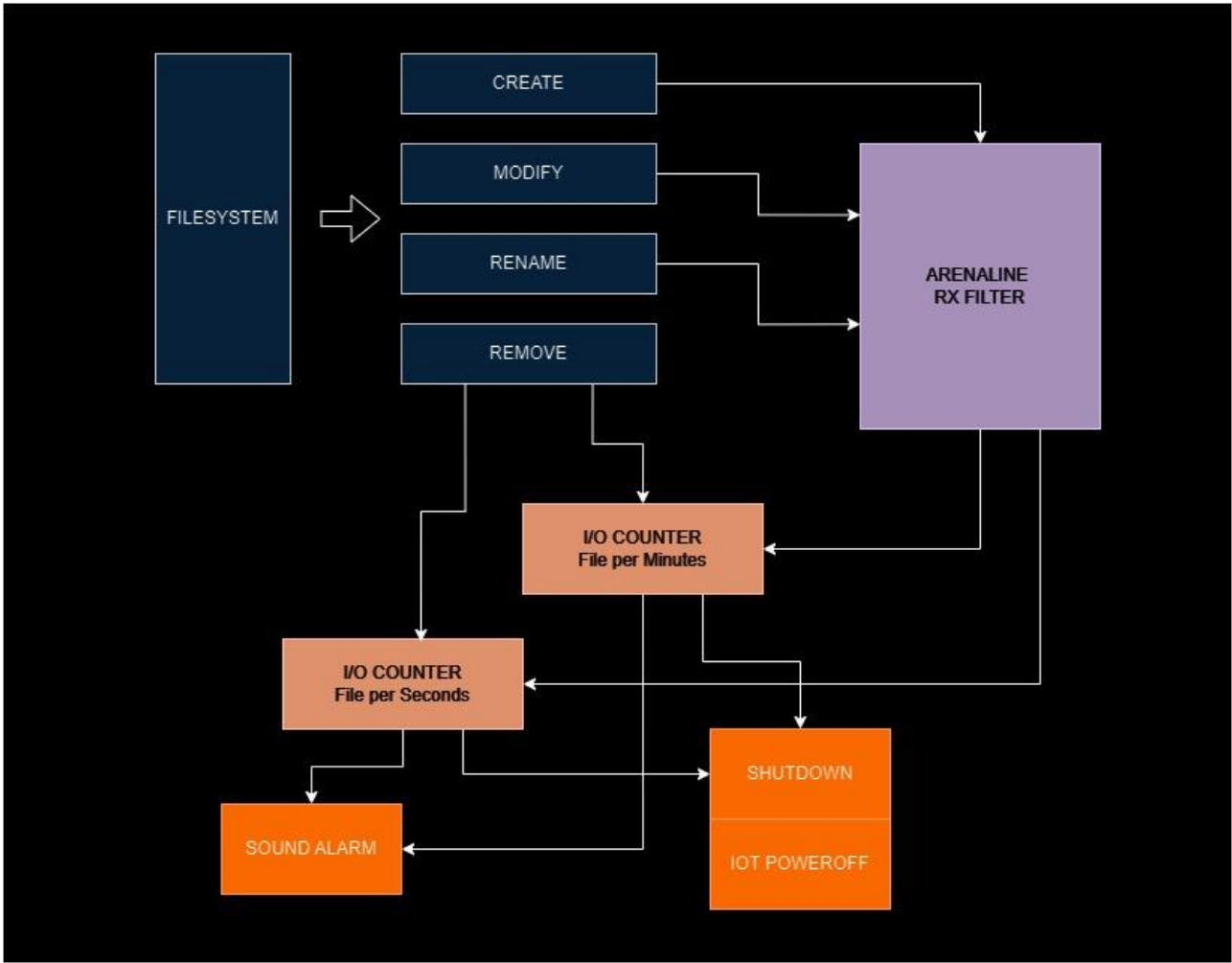
Tutti i valori sono espressi al minuto/secondo(*)).



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

*I file che Adrenaline ha reputato puliti non risulteranno nei contatori

Adrenaline RX AntiRansomware Filter:



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.