Adrenaline RX (Anti-Ransomware / File-Monitor)

Document Version: 0.0.1.5

Software Version: 3.5.0200.1

ADRENALINE RX USER GUIDE

Introduction

The proliferation of ransomware represents one of the most serious threats to contemporary computer security. Ransomware encrypts the victims' data, demanding a ransom for their decryption. Traditional security measures, such as antivirus and firewalls, are often insufficient to counter these constantly evolving threats.

AdrenalineRX is based on a combination of advanced analysis techniques to detect and prevent ransomware attacks.

Architecture and Operation of AdrenalineRX

AdrenalineRX examines every file created in the system such as: file entropy, name entropy, magic bytes, file extension, file IO flow, and canary file management.

File Entropy

The entropy of a file is a measure of the disorder or randomness in the data contained in the file itself. In general, an encrypted file has significantly higher entropy compared to an unencrypted file. AdrenalineRX calculates the entropy of each file to identify potential encryption activities. If the entropy exceeds a predefined threshold, the file is marked as suspicious.

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

Magic Bytes

The term "magic bytes" refers to the presence of characteristic byte sequences at the beginning of files that identify the file type. These sequences, also known as "magic numbers", are used by AdrenalineRX to verify the consistency between the file content and its declared extension.

File IO Flow

AdrenalineRX analyzes in real time the input/output operations of files in the filesystem, focusing on creation, modification, renaming, and deletion operations. An anomalous increase in these activities can be indicative of a ransomware that is encrypting files.

Canary Files

AdrenalineRX also uses canary files as a detection method. Canary files are specially created and monitored files that should never be modified during normal system use. Any attempt to access, modify, or delete these files immediately triggers an alarm.

Synergy of Detection Techniques

The strength of AdrenalineRX lies in the synergistic combination of these parameters. Each technique provides a piece of the puzzle, and together they form a highly effective detection system. The multi-parametric approach allows to reduce false positives and increase detection accuracy. AdrenalineRX not only identifies suspicious files, but also the overall system behavior, allowing a timely and targeted response to threats.
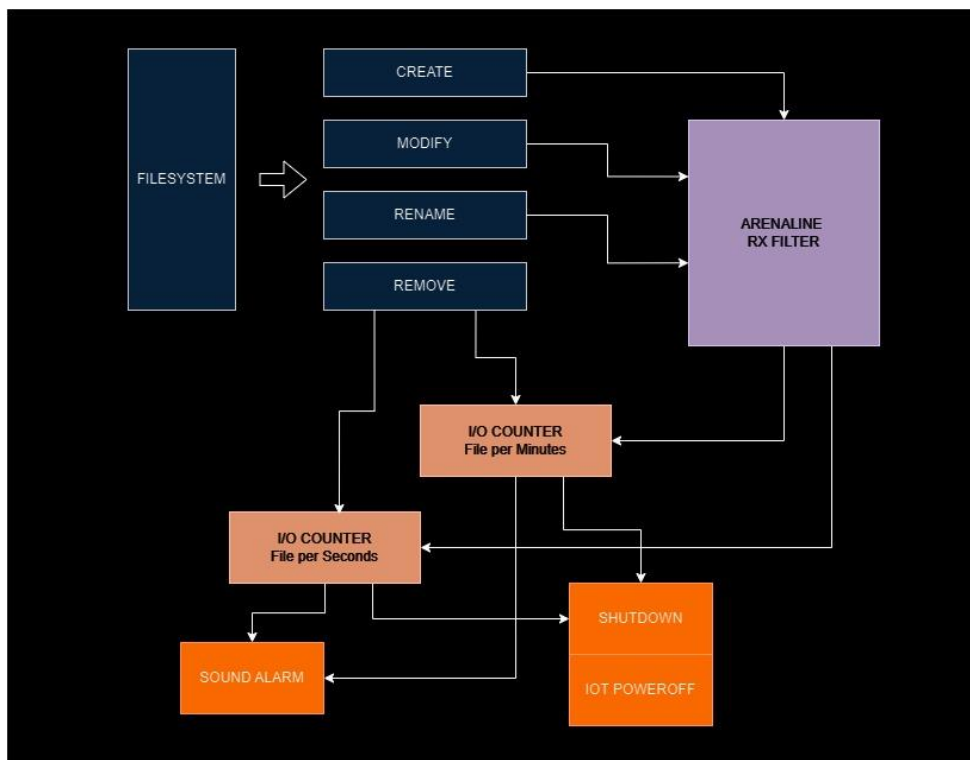
Extreme Containment Actions

AdrenalineRX is designed as the last line of defense against ransomware attacks. In the event that an attack manages to bypass the initial detection measures and begins to encrypt files, AdrenalineRX is capable of executing extreme containment actions. Among these, the most drastic is the immediate shutdown of the system. Shutting down the system can interrupt the encryption process, reducing damage to files not yet compromised.

This function is particularly useful when all other defense measures have failed.

Startup

After being started, AdrenalineRX displays a series of initial data to understand the status of the program and its current configuration. This data provides detailed information on active settings and features, including the type of log used, the status of the shutdown function, the file monitoring path, and alarm settings for file creation, modification, renaming, and removal operations.
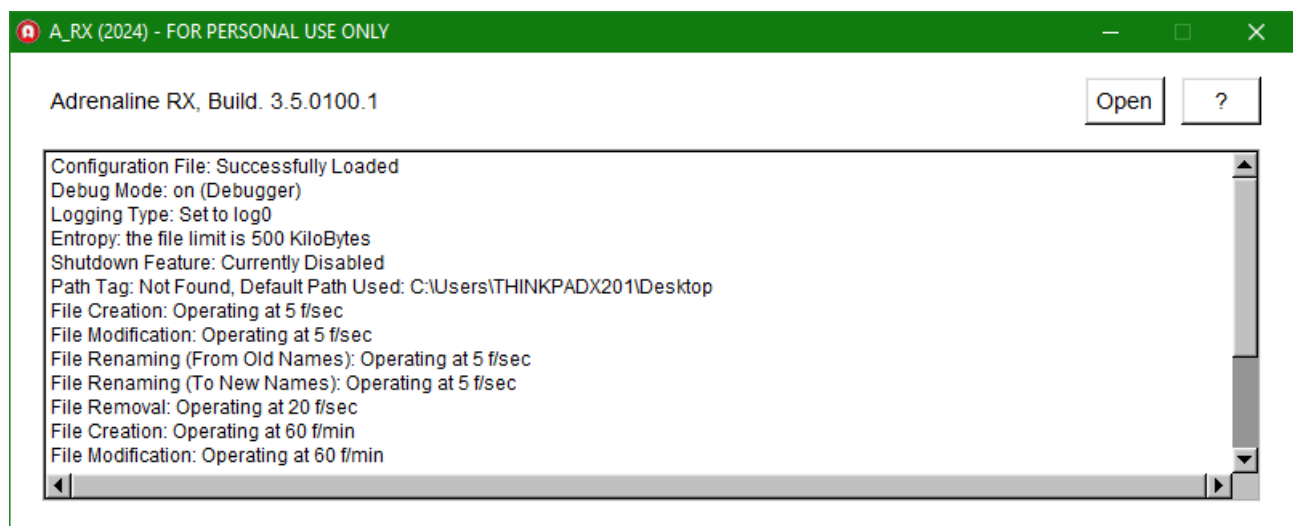
Sound Alarm

When AdrenalineRX detects suspicious or potentially harmful activity, it activates a sound alarm to promptly alert the user of the ongoing anomalous activity. The sound alarm is designed to immediately capture the user's attention and signal the presence of a potential system security risk, and is primarily used for fine-tuning activities.

The "ALARM.wav" file, located in the root folder of AdrenalineRX, contains the alarm sound used for this specific purpose. This audio file is designed to be easily recognizable and distinctive, ensuring that the user can quickly identify the alert of a potential threat.

Sound alarms play a fundamental role in the analysis and testing phases before AdrenalineRX goes into actual production. During this phase, developers and security analysts use sound alarms to verify the system's effectiveness in detecting and reporting suspicious activities. This process allows for the evaluation of the system's reliability and the implementation of any necessary optimizations or improvements before AdrenalineRX is deployed in a production environment.

Automatic Shutdown

When AdrenalineRX identifies harmful activity, it can automatically initiate the system shutdown function to prevent further damage and safeguard data integrity. This automatic shutdown feature is designed to promptly intervene in critical situations, protecting the system and data from the expansion of damage caused by malicious activities.

Magic Bytes Configuration File (magic.cfg)

In the configuration file, each line specifies a file type with its corresponding extension and the corresponding "Magic Byte" used to identify the file type. Magic bytes are unique byte sequences that are found at the beginning of a file and are used to determine its type or format. These values are then used by Adrenaline to correctly recognize and handle different file types during analysis and protection operations.


```
magic.cfg - Blocco note di Windows
File  Modifica  Formato  Visualizza  ?
.zip 50 4B
.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
```

Installation

To configure Adrenaline Rx, follow these steps carefully:

1- Start Adrenaline Rx: After installing the program, start it by double-clicking on the application icon.

2- Initial Configuration: Adrenaline Rx will open with default values. It will start monitoring the default directory, usually C:/Users/user/Desktop.

3- Open the configuration file: To customize the settings, press the "Open" button from the Adrenaline Rx interface. This will allow you to access the configuration file, usually called config.cfg.

4- Modify the settings: Using a text editor, open the config.cfg file and modify the settings according to your needs. You can specify the paths to monitor, adjust the detection settings, and more.

5- Save and close: Once the changes have been made, save the config.cfg file and close the text editor.

6- Restart Adrenaline Rx: To apply the changes, close and restart Adrenaline Rx. In this way, the program will use the new settings configured in the config.cfg file.

By following these steps, you can customize the settings of Adrenaline Rx and configure the program to adapt it to your specific computer security needs.

Configuration File (config.cfg)

The Adrenaline configuration file (config.cfg) contains the main settings of the program, such as the type of log, the status of the shutdown function, the monitoring path, and the thresholds for the file alarm.

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.
```

Note: It's important to note that commands are case-sensitive, so make sure to correctly respect the syntax when modifying the configuration file.

List of commands that you can configure within the config.cfg file::

Command: LOG=<log0 | log1>

Used for: Fine-Tuning / File Tracking

The log file, essential for tracking activities and for optimizing performance, is generated daily and can be found in the main directory of Adrenaline, specifically in the ".\log" folder.

log0: This recording mode is inactive, not recording any event.

log1: Enable this mode to view the files processed by AdrenalineRX. This mode is particularly useful for understanding the "noise" generated by reading the filesystem. If you notice that there are files or folders that are being read but should not be included in the process, you can adjust your exclusion settings to ignore these files or folders in the future. In this way, the logs help you optimize the performance of AdrenalineRX, reducing the time spent reading unnecessary files or folders and improving the efficiency of your process. Remember, however, that any changes to the exclusion settings should be made with caution, to avoid accidentally excluding important files or folders.

Command: IO_MONITOR=<on|off>

Used for: Fine-tuning

This mode allows you to display the number of files per second and per minute, providing useful information to correctly adjust the threshold values in alarm triggers.

The IO_MONITOR mode automatically deactivates after 100 detections, ensuring that it is not excessively used.

The use of the IO_MONITOR mode is valuable because it allows users to better understand the filesystem activities per second and per minute, and to accurately adjust the parameters of the alarm triggers to adapt them to their specific security needs.
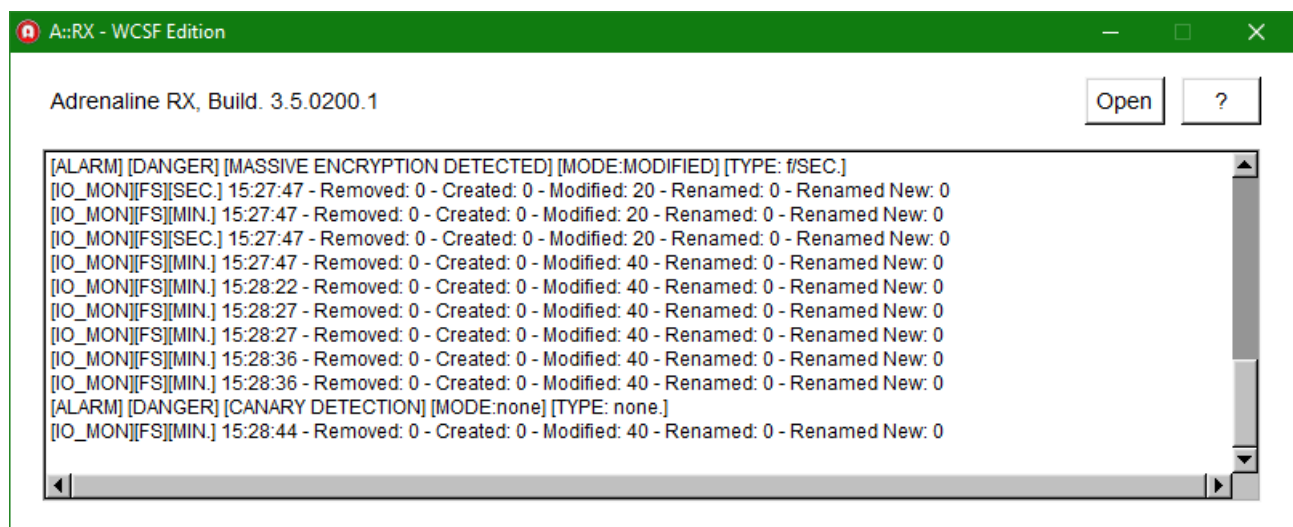
In this example (image above)

- The "Removed" counter keeps track of all deleted files, while the other parameters are filtered through Adrenaline RX algorithms.

- Files that Adrenaline RX filters have deemed clean will not appear in the counters.

Command: POWER=<on|off>

Used for: Last Defense

The POWER command enables or disables the computer shutdown function in response to a critical alarm detected by the antiransomware. When this function is enabled, the system will automatically shut down after the antiransomware has detected a critical alert, such as a mass encryption attempt by ransomware.

This automatic shutdown mechanism is designed to limit damage in the event of a ransomware attack. When suspicious or harmful activity that could compromise data security is detected, the antiransomware triggers the critical alarm and, if the automatic shutdown function is enabled, the computer immediately shuts down to prevent further damage.

This is an important defense tool to protect sensitive data and prevent the spread of ransomware in the system, allowing users to respond promptly and limit the impact of cyber attacks. However, it is important to use this function with caution, as shutting down the computer interrupts all ongoing activities.

TIPS: *Enable the "POWER=on" command only when you are sure you have configured the exclude.cfg file.*

Command: PATH=<path>

Used for: Filesystem reading

This command specifies the path where the monitor begins scanning in recursive mode, checking all subdirectories within the specified path.

If the PATH path is not correctly defined, AdrenalineRX uses the default path which is C:\Users\user\Desktop

You can also use drive letters like C:, but this generates a lot of noise. To reduce the noise, you need to configure the exclude.cfg file by adding the noisy paths to exclude from monitoring.

Command: FILE_LIMITER=<KiloBytes>

Used for: Entropy Frame Limiter.

This command determines the size of the first data segment, or "frame", that the entropic engine analyzes.

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>

These commands allow you to set the trigger for filesystem-related alarms, expressed in seconds/minute. When a value is specified, Adrenaline RX monitors the number of files created in the system every second/minute.

If the number of files exceeds the specified value, an alarm is triggered.

If a value of zero is set (e.g., CREATE=0), then the parameter is not evaluated.

For example, if you set CREATE=4 in the config.cfg file and 5 files are created in a second, Adrenaline RX will reevaluate the score of the internal filter to signal high file creation activity.

Command: REMOVE=<files per second>

            REMOVE_M=<files per minute>

These commands set the trigger for file removal alarms, expressed respectively in seconds and minutes. When a value is specified, Adrenaline RX monitors the number of files removed from the system in the corresponding time period. If the time elapsed from the removal of a file exceeds the specified value, an alarm is triggered.

However, it is crucial to carefully evaluate the use of these commands when configuring monitoring paths, especially if you are monitoring operating system paths or other high-noise directories. For example, if you are monitoring the system files of the operating system, frequent file removals may occur that are not necessarily indicative of an attack or suspicious behavior. In these cases, activating time-based alarms could generate false positives and create confusion.

Therefore, it is advisable to carefully evaluate the configuration of file removal triggers, taking into account the operational context and the specific characteristics of the system. You can reduce the risk of false positives by adjusting the trigger values based on the expected frequency of file removal in the specific context of monitoring. This allows you to maintain a balance between the sensitivity of the alarm system and the reduction of false positives, ensuring that alerts are genuine and relevant to the system's security.

To optimize the configuration of file removal triggers, it is advisable to use the IO_MONITOR mode to closely monitor system activity. This allows you to accurately assess the frequency of file removals and calibrate the triggers in the config.cfg file appropriately. The use of the IO_MONITOR mode allows you to adapt the triggers based on the operational context and the specific characteristics of the system, minimizing the risk of false positives and ensuring that alerts are genuine and relevant to the system's security.

Command: MAX_CANARY_ALARM=<file_per_session>

The MAX_CANARY_ALARM command allows you to specify the maximum number of Canary files that can be mistakenly manipulated by the user before an alarm is triggered. This setting defines an error threshold for the alarm system with respect to Canary files and counts for the entire duration of the Adrenaline RX session, regardless of the active filters.

For example, if you set MAX_CANARY_ALARM=2, it means that at least two Canary files must be manipulated during the entire session of using Adrenaline RX before an alarm is triggered.
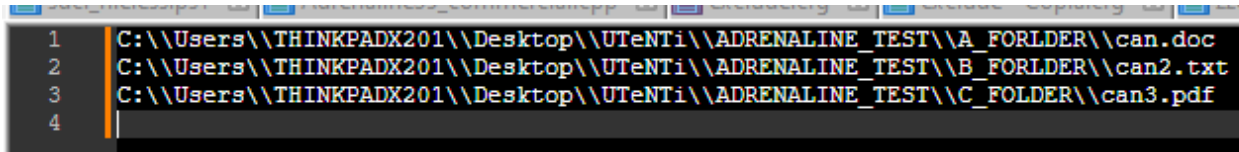
Command: CANARY_HIDE=<on | off>

Recommended value: off

When the CANARY_HIDE flag is set to "on" and Canary files are generated with the "hidden" attribute, they will not be visible within File Explorer in Windows, unless the user has activated the "Show all hidden files" option.

File canary.cfg :

Canary.cfg contains the paths and the name of the files that are generated by 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>

The ENTROPY command in the Adrenaline RX configuration file allows you to adjust the minimum entropy parameter. This parameter defines the minimum entropy threshold that a file must have in order to be considered potentially suspicious or harmful.

Exclude paths:

One of the features of Adrenaline RX is the ability to exclude certain file paths from scans, to avoid false positives or to improve performance during analysis.

This is particularly useful for paths that contain system files or application data that do not require monitoring.

Editing the exclude.cfg File

To configure path exclusions in AdrenalineRX, you need to edit the exclude.cfg file, located in the program's configuration directory.

```
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.
- The configuration files are typically found in the AdrenalineRX installation folder. Press the "**Open**" button to reach the installation folder.
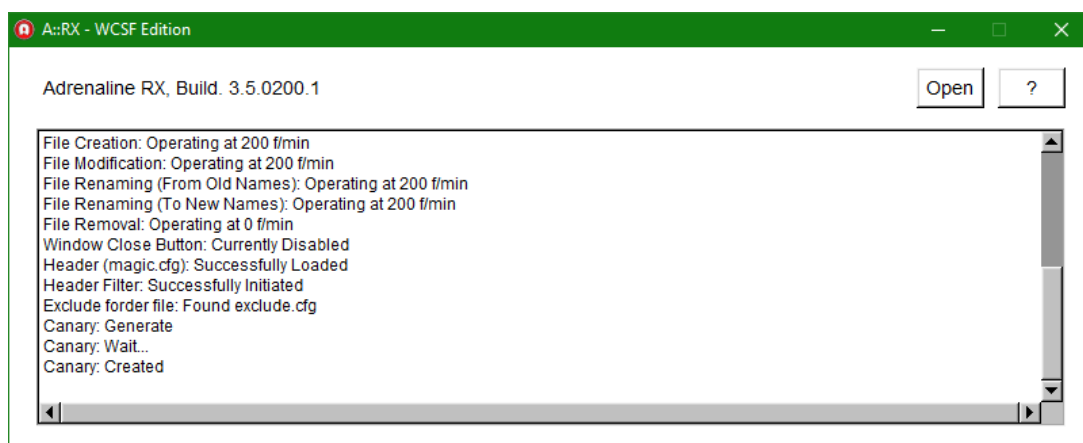
2- Open the File for Editing:

- Use a text editor like Notepad or Notepad++ or any other preferred text editor to open exclude.cfg.

Versioning Scheme

The versioning system of Adrenaline Rx follows a standard scheme composed of four numbers:

• Main Version: Indicates a significant version of the software with major changes or additions of features.

• Major Revision: Represents a smaller revision compared to the main version, generally characterized by significant improvements or important updates.

• Minor Revision: Indicates a smaller revision compared to the major revision, which includes minor adjustments, bug fixes or performance improvements.

• Bug Number: Represents the number of bugs fixed from the version.

For example, consider the version "3.5.0100.0":

• "3" is the main version.

• "5" is the major revision.

• "0100" is the minor revision.

• "0" indicates the number of bugs fixed.