

Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

Title of Work: Malware-Prevention-Method

Author: Anvar Kutlimuratov

Year of Creation: 2009

Full Description of the Work

1. Introduction

Modern malware is becoming increasingly sophisticated, and traditional antivirus systems often fail to provide effective protection. This document presents the **Malware-Prevention-Method**, which is based on **modifying file extensions to prevent malware execution on the system**. This method was developed as **an alternative approach to traditional antivirus solutions** and has been tested in practice since 2009.

2. Working Principle

This method operates on the following principles:

1. **Changing file extensions** – Modifying the extension of executable files from the standard `.exe` format to a different format, such as `.123`.
2. **Blocking execution at the system level** – Since malware typically relies on `.exe` files, if the system does not recognize `.exe` files as executable, the virus will fail to launch.
3. **Monitoring system activity** – If malware attempts to restore the `.exe` extension, the system does not recognize it and prevents execution.
4. **User-controlled execution** – Only trusted applications can be executed with the modified extension (`.123`).

3. Difference from Traditional Methods

Traditional antivirus programs detect malware using the following approaches:

- **Signature-based detection** – Identifying malware based on known virus signatures.
- **Behavior-based analysis** – Detecting suspicious activity during program execution.
- **Sandboxing technology** – Running files in an isolated environment to observe behavior.

This method, however, **does not attempt to detect malware but instead prevents its execution entirely**.

4. Capturing Undetectable New Viruses

Traditional antivirus systems struggle to detect **zero-day attacks** and **polymorphic viruses**. The **Malware-Prevention-Method** forces such viruses to expose themselves because they rely on `.exe` execution. If the virus tries to restore the `.exe` extension, the system immediately

prompts the user for an execution method. This allows users to **detect and prevent suspicious activity instantly**.

This approach can be a **powerful tool for detecting and preventing new and unknown viruses** by creating a universal security barrier against all malware.

5. Practical Applications

This method can be applied in the following areas:

- **Corporate IT security** – Protecting internal networks from malware threats.
- **Personal computer users** – Enhancing security for individual users.
- **Cloud services and servers** – Safeguarding cloud environments and server infrastructures from malware.

6. About the License

This work is distributed under the **Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License**.

<https://creativecommons.org/licenses/by-sa/4.0/>