

Forum:[Hack Forums](#)

Thread: [\[MRT-X Academy\] REM-VBS Worm Tutorial](#)

Tha Sneak - February 16, 2025, 8:14 pm

Rem-VBSWorm Tutorial

Rem-VBSWorm is a portable tool designed to remove VBS (Visual Basic Script) malware, worms, and autorun-based infections. This tool specifically targets VBS infections that may not be detected by standard antivirus programs and helps users clean infected drives and USB devices.

1. What is Rem-VBSWorm?

Rem-VBSWorm is a lightweight, user-friendly application developed to detect and remove VBS worms and malicious scripts that spread through USB drives and other removable storage devices. It helps disinfect compromised systems and USB devices and also repairs changes made by the malware to system settings.

It can also restore hidden files that were altered by the worm and delete suspicious autorun files.

2. Downloading Rem-VBSWorm

Follow these steps to download Rem-VBSWorm: Visit the official download page: [Rem-VBSWorm on SourceForge](#).

Download the latest version of the tool from the page.

Save the file to your Desktop or another easily accessible folder.

3. Preparing to Use Rem-VBSWorm

Before running Rem-VBSWorm, make sure to disable your antivirus temporarily, as some antivirus software may flag the tool as a potential threat (due to the tool interacting with autorun files and VBS scripts). Once the tool is downloaded: Disable real-time protection in your antivirus software temporarily to avoid interruptions during the scan.

You can re-enable the antivirus after completing the scan and cleanup process.

4. Running Rem-VBSWorm

To run Rem-VBSWorm, follow these steps: Locate the downloaded Rem-VBSWorm executable file.

Double-click the file to launch the application.

Rem-VBSWorm will open a simple interface with a few key options to scan and clean your system.

Insert any USB drives that you suspect might be infected.

5. Using Rem-VBSWorm to Scan and Clean

Once the tool is open, you can start the scanning process: Click on the “Scan” button to begin scanning your system and USB drives for any VBS worms or autorun infections.

The tool will analyze both the system and any connected USB drives to detect malicious scripts and autorun files.

Rem-VBSWorm will show a list of infections if any are found.

To clean the infections, simply click on the “Clean” button. The tool will delete the detected threats.

During the scan, Rem-VBSWorm will: Remove autorun.inf files created by VBS worms.

Restore hidden files on the USB drives that were hidden by malware.

Clean VBS script infections from the USB drives and system folders.

6. Additional Features of Rem-VBSWorm

In addition to its scanning and cleaning capabilities, Rem-VBSWorm offers several helpful options: **Unlock Folders:** If the malware has locked or hidden your folders, Rem-VBSWorm can unlock and unhide them.

Restore System Settings: Some VBS worms modify system settings to disable Task Manager, Registry Editor, or Folder Options. Rem-VBSWorm can restore these settings to their default state.

Backup and Restore: The tool provides options to back up important files before cleaning infections and restore files if necessary.

7. After Cleaning – Preventing Future Infections

After cleaning your system and USB drives using Rem-VBSWorm, follow these steps to protect yourself from future infections:

Enable Your Antivirus: Re-enable real-time protection in your antivirus software to ensure your system remains protected.

Disable Autorun on USB Devices: VBS worms often spread through the autorun feature on USB drives. Disabling autorun will help prevent future infections. To disable autorun: Press Windows + R, type gpedit.msc, and press Enter.

Navigate to Computer Configuration > Administrative Templates > Windows Components > AutoPlay Policies.

Double-click Turn off AutoPlay, enable the policy, and apply it.

Scan USB Drives Regularly: Always scan USB drives before using them, especially if they have been connected to other systems.

8. Conclusion

Rem-VBSWorm is an effective, easy-to-use tool that helps you detect and remove VBS worms, autorun infections, and malicious scripts from your system and USB drives. By running regular scans with Rem-VBSWorm and keeping your antivirus software updated, you can protect your system from these threats.

Download Rem-VBSWorm here: [Rem-VBSWorm on SourceForge](#)

Tha Sneak - February 19, 2025, 3:44 pm

Tha Sneak - March 1, 2025, 8:43 pm

Please do NOT reply to this thread in case information needs to be added or edited.

If you have a questions about the contents of the thread or other tutorials please go to this thread and post your question in this thread: <https://hackforums.net/showthread.php?tid=6293473>

Thanks,

Tha Sneak

