Mal.EDU v0.3 - ‘Yellow’ Quickstart Guide

Use this guide for installing or reinstalling the program.

Introduction

This guide provides instructions on how to reset and replant Mal.EDU after an exercise. Please follow the steps carefully to ensure a successful setup.

- Note: If you are upgrading from v0.2a, be sure to delete all traces using 0.2a’s uninstaller. From there, you may continue v0.3’s setup.

Prerequisites

- Ensure you have administrative access to your computer.
- A USB stick to transfer the files from a computer with wifi to the exercise computer
  - Alternately, an active internet connection on the exercise computer (not recommended)

Steps

Step 1: Preparation

1. **Open and download on a separate PC** - Navigate to the Mal.EDU setup page on GitHub - Go to Mal.EDU Setup Page.

   If you are viewing on paper: (https://github.com/StrataBytes/Mal.EDU/tree/main/v0.3%20'Yellow'/CCIC/Start)

2. **Download Necessary Files** - From the page, download the following files:
   - `csrssQ.exe`
   - `start.bat`
   - `removeMalEDU.bat`

3. **Move the files to a USB stick -**
   - Now that you have everything on a USB stick, you may move to the next.

Step 2: Clean Existing Installation

1. **Run `removeMalEDU.bat` File** - Execute the `removeMalEDU.bat` file **AS ADMINISTRATOR** to clear any previous configurations.
    a. Note: Ignore any errors that may appear during this process.

Step 3: Setup New Environment

(Note, this is an example - you may configure it how you like, this just works.)

1. **Navigate to Directory** - Open File Explorer and go to `C:\Users\YOUR_USER\AppData\Roaming\Microsoft`. Replace `YOUR_USER` with your actual username.
2. **Create a New Folder** - Right-click and select `New > Folder` to create a new folder named `Essential` or any other discreet name you prefer.
3. **Move `csrssQ.exe` From the USB Stick** - Place the `csrssQ.exe` file into the newly created folder. Remember to copy the full path to this file for later use.
    a. Fun fact; csrssQ.exe is a real windows service for the Client/Server Runtime Subsystem! This may have a tiny chance to trick the technician if they do a google search before annihilating it!

Step 4: Finalize Setup

1. **Execute `start.bat` as Administrator** - Right-click on `start.bat` and choose `Run as administrator`. You can do this from any location, such as the USB stick.
2. **Enter csrssQ.exe Path** - When prompted, paste the full path to the `csrssQ.exe` file you copied earlier, ensuring it includes `csrssQ.exe` at the end.
3. **Setup Timing** - Select `1 min` when asked for the time.
4. **Complete Setup Script** - Follow any remaining on-screen instructions to complete the setup.

Step 5: Cleanup

1. **Delete Setup Files** - Ensure you delete the `start.bat` and `removeMalEDU.bat` files if you put them on the computer. If they are still on the USB stick, you are fine.
2. **Close Open Windows** - Check for and close any open windows or tabs related to the setup process to leave no trace. This also includes **RUN COMMAND HISTORY.**

Optional Steps:

Disable Task Manager

You can disable the task manager to make things more difficult. On the Github page, there will be some registry files. Chose the one that is labeled something around the lines for “Task Manager Disabled”. Then, load that file using regedit.
Be sure to back up your previous registry before doing this!

Hide `csrssQ.exe` from Task Manager Startup Apps

- **Caution:** This step is optional and not recommended due to potential issues. If desired, you can attempt to hide `csrssQ.exe` from Task Manager's startup apps. However, be aware that Windows may prevent the program from starting if it's hidden.

Download Python

- This also will not add much, however if your anti-virus is flagging Mal.EDU, downloading python to PATH could help.

Unplugging from ethernet / wifi

- Windows defender is extra insane when the system is online or once it has updated from a fresh install of windows. Disconnecting will help it from interfering.

Adding exceptions to windows defender

- Adding exceptions for Mal.EDU’s csrssQ.exe file in WD will stop it from deleting or quarantining Mal.EDU if it is being a thorn in the side, but doing so will point directly to the file location.

Conclusion

You have successfully completed the setup for Mal.EDU v0.3 - ‘Yellow’. If you encounter any issues or have questions, please let me know.

Disclaimers

Mal.EDU is strictly designed for a controlled setting on consented systems. Do not use it for malicious intentions.
Mal.EDU is also not responsible for any damage. Use this program and guide ‘as is’.

Author: Stratabytes