|  |  |
| --- | --- |
| **Topic:** | Kill MSRA remotely |

Use Care:  
Script used to terminate applications or processors and reboot devices remotely, useful for countering malware or faulty applications making remote connections difficult.

Requirements:

* Set-executionpolicy -executionpolicy unrestricted
* Host machine must be on the company network.

Process:

This PowerShell script is a remote administration tool that allows you to perform various tasks on remote devices. Here’s a step-by-step guide on how to use it:

1. **Open PowerShell**:
   * Open PowerShell on your Windows machine.
2. **Run the Script**:
   * Navigate to the directory where the script is located.
   * Run the script by typing .\Remote\_Admin.ps1 and pressing Enter.
3. **Main Menu**:
   * The script will display a menu with the following options:

Remote Admin Tool

1. Reboot a remote device

2. Check services on a remote device

3. Kill a process on a remote device

4. Exit

1. **Choose an Option**:
   * Enter the number corresponding to the task you want to perform and press Enter.

**Options Explained:**

1. **Reboot a Remote Device**:
   * Enter [1](vscode-file://vscode-app/c:/Users/e103719/AppData/Local/Programs/Microsoft%20VS%20Code/resources/app/out/vs/code/electron-sandbox/workbench/workbench.html) and press Enter.
   * You will be prompted to enter the computer name of the remote device.
   * The script will then attempt to reboot the specified remote device using the [shutdown](vscode-file://vscode-app/c:/Users/e103719/AppData/Local/Programs/Microsoft%20VS%20Code/resources/app/out/vs/code/electron-sandbox/workbench/workbench.html) command.
2. **Check Services on a Remote Device**:
   * Enter [2](vscode-file://vscode-app/c:/Users/e103719/AppData/Local/Programs/Microsoft%20VS%20Code/resources/app/out/vs/code/electron-sandbox/workbench/workbench.html) and press Enter.
   * You will be prompted to enter the computer name of the remote device.
   * The script will retrieve the list of services running on the remote device and export it to a CSV file in the script's directory.
3. **Kill a Process on a Remote Device**:
   * Enter [3](vscode-file://vscode-app/c:/Users/e103719/AppData/Local/Programs/Microsoft%20VS%20Code/resources/app/out/vs/code/electron-sandbox/workbench/workbench.html) and press Enter.
   * You will be prompted to enter the computer name of the remote device.
   * The script will display a sub-menu with the following options:

Remote process termination function

BE CAREFUL WITH THIS FUNCTION

To output processors type 1, to kill a process using pid type 2, to kill a process using name type 3, to close type exit

* + Enter the number corresponding to the action you want to perform:
    - [1](vscode-file://vscode-app/c:/Users/e103719/AppData/Local/Programs/Microsoft%20VS%20Code/resources/app/out/vs/code/electron-sandbox/workbench/workbench.html): Display the list of processes running on the remote device.
    - [2](vscode-file://vscode-app/c:/Users/e103719/AppData/Local/Programs/Microsoft%20VS%20Code/resources/app/out/vs/code/electron-sandbox/workbench/workbench.html): Kill a process by its process ID.
    - [3](vscode-file://vscode-app/c:/Users/e103719/AppData/Local/Programs/Microsoft%20VS%20Code/resources/app/out/vs/code/electron-sandbox/workbench/workbench.html): Kill a process by its name.
    - [exit](vscode-file://vscode-app/c:/Users/e103719/AppData/Local/Programs/Microsoft%20VS%20Code/resources/app/out/vs/code/electron-sandbox/workbench/workbench.html): Exit the sub-menu and return to the main menu.

1. **Exit**:
   * Enter [4](vscode-file://vscode-app/c:/Users/e103719/AppData/Local/Programs/Microsoft%20VS%20Code/resources/app/out/vs/code/electron-sandbox/workbench/workbench.html) and press Enter to exit the script.

**Notes:**

* Ensure you have the necessary permissions to perform these actions on the remote devices.
* Use the script with caution, especially the process termination function, as it can disrupt services on the remote device.