Modifying Windows 10 Build 1511
For Privacy And Stability

Author: @actrons @k1ttens

15-10-2017

1   The Road To Amelioration

This article will go over how to remove most of the junk, spyware, and anti-trust violations that come with a stock windows 10 install in other words this article serves to describe a "fix" for Windows 10. As of the writing of this article only Windows 10 version 1511 can be fixed. The means you will be stuck without updates which is a problem that will need to be taken into consideration at a later date, right now it needs to be made possible on at least the first general released version of Windows 10. If you need security, DO NOT use Windows this is more of a patch than a solution.

Firstly You will need a Windows 10 Build 1511 image which has been obtained from Microsoft. You will need to extract this provided image:

https://actrons.info/files/Windows_10_1511_AMD64.tar.gz

You will not be needing a key for this and any 1511 version of windows will do (Home, Professional, Enterprise, N version of windows) Enterprise and N versions have not been tested but the process should work just the same.

Secondly you will need a live GNU/Linux image and either another USB flash drive or you can re-use the one used to install Windows with when you are done with installing Windows. Ubuntu 16.04 is recommended. You can use whatever means desirable to write the linux iso to the USB flash drive (dd, rufus, etcher, etc.)

You will also be in need of a script or a list of commands that will disable many unwanted Windows 10 "features". The script is provided here:

https://actrons.info/files/win10.html

2   The Initial Deletion Process

Because of the changes that we will be performing to the Windows 10 installation, the operating system cannot be actively running, as certain permissions for the concerning files are missing, and Windows initiated repairing operations may occur. This requires the operating system to be shut down, and it's file-system mounted in another OS, preferably a Linux distro, after an initial install and configuration using the provided script has been completed.

2.1   Installation

2.1.1   Write the Windows 10 ISO to a USB flash drive (8GB or larger) using a disk writing tool that supports making bootable drives.

2.1.2   Copy the setup script and zip file from above onto the flash drive.

2.1.3   Disconnect the target machine from the Internet, removing the Ethernet cord if necessary.

2.1.4   Turn on the target machine and boot from the USB drive with Windows 10 Build 1511 image.

2.1.5   Before the install begins it will ask for a license key, click "I do not have one" and continue the install process. The machine will reboot a few times before it has completed

2.1.6   When the target boots for the first time fully it will prompt the user to either continue with the default settings or as noted near the bottom of the page there is a hyperlink to customize these settings. Disable all of the settings on the following pages.

2.1.7   The last bit of information it asks for is a Username and Password, After this is done some very informative text fades in and out, thus lulling the user into a coma before Windows finally displays the desktop.

2.1.8   Copy the script and zip file from the install USB to the desktop.

2.1.9   Right click the script and click Run as Administrator.

2.1.10   Run options 1,3, and 5 following the on screen instructions. During the first step you will be asked to connect to the Internet, do so.

2.1.11   When steps 1,3, and 5 have been completed shutdown the computer.

2.1.12   Turn on the machine and boot from the Linux Live USB flash drive. With Ubuntu run with the first option (Try Ubuntu without installing).

2.1.13 Mount the Windows disk, with Ubuntu it should simply be on the sidebar.

2.1.14 Delete the following files and folders from the Windows hard drive (You will have to search for these files either by using command line or the search functionality of Ubuntus' Nautilus file manager):

1. //Program Files/Internet Explorer
2. //Program Files/WindowsApps
3. //Program Files/Windows Defender
4. //Program Files/Windows Mail
5. //Program Files (x86)/Internet Explorer
6. //Program Files (x86)/Windows Defender
7. //Program Files (x86)/Windows Mail
8. //Windows/InfusedApps/Applications
9. //Windows/InfusedApps/Package
10. //Windows/SoftwareDistribution/SIH*
11. //Windows/System32/AppxDeploymentServer.dll
12. //Windows/System32/storewuauth.dll
13. //Windows/System32/SIHClient.exe
14. //Windows/System32/en-US/sihclient.exe.mui
15. //Windows/System32/wusa*
16. //Windows/System32/WUDF*
17. //Windows/System32/wua*
18. //Windows/System32/wups*
19. //Windows/SystemApps/...CloudExperienceHost...
20. //Windows/SystemApps/...ContentDeliveryManager...
21. //Windows/SystemApps/ContactSupport*
22. //Windows/SystemApps/Microsoft.MicrosoftEdge*
23. //Windows/SystemApps/Microsoft.Windows.Cortana*
24. //Windows/SystemApps/Microsoft.XboxGameCallableUI*
25. //Windows/SystemApps/Microsoft.XboxIdentityProvider*
26. //Windows/SystemApps/WindowsFeedback*
27. //Windows/SysWOW64/OneDriveSettingSyncProvider.dll
28. //Windows/SysWOW64/OneDriveSetup.exe
31. //Windows/SysWOW64/wuapi.dll
32. //Windows/SysWOW64/wuapi.dll.mui
37. //Windows/diagnostics/system/Apps
38. //Windows/diagnostics/system/WindowsUpdate

2.1.15 Search the entire Windows drive for each of the search terms listed below and follow the instructions

Search term (nautilus search results)	Instructions	Notes
applocker	delete everything	
apprepsync	delete everything	
AutoLogger	delete everything	
clipup	delete everything	
clipsvc	delete everything	
cortana	delete everything	
diagtrack	delete everything	
DeliveryOptimization	delete everything	
dmclient	delete everything	
EnhancedStorage	delete everything	
hotspot	delete everything	skip immersivecontrolpanel items
homegroup	delete everything	
invagent	delete everything	
maps	delete everything	skip immersivecontrolpanel items
msra	delete everything	
serviceinitiatedhealing	delete everything	
SIHClient	delete everything	
slui	delete everything	
startupscan	delete everything	
usoclient	delete everything	
usocore	delete everything	
windowsupdate	delete everything	
wsqmcons	delete everything	
wua	delete everything	
wus	delete everything	
wusa	delete everything	

Table 1: Overview of services to delete

2.1.16 Shutdown Ubuntu, remove the Ethernet cable and reboot into Windows

2.1.17 When you have reached the desktop type "*taskschd.msc*" and press enter to run Task Scheduler

2.1.18 Expand the Folders under Task Scheduler Library until you see a long list of folders

2.1.19 Delete the tasks under the following folders (the Application Experience folder is not removable by the user):

1. AppID -delete only- Policy Converter and VerifiedPublisherCertStoreCheck
2. AppxDeploymentClient
3. Application Experience
4. Clip
5. Customer Experience Improvement Program
6. Feedback
7. Maps
8. UpdateOrchestrator (has no effect across reboots, no detrimental effects)
9. Windows Defender
10. WindowsUpdate (has no effect across reboots, no detrimental effects)
11. WS

2.1.20 Reboot once more for good measure, plug in Ethernet/connect to the Internet

3   Tying Up Loose Ends

Some things to clean up after you reboot into the new install of Windows 10. A shortcut to Edge remains in the taskbar, simply right click an un-pin. Many of the pre-installed apps will still have their shortcuts remaining in the default Windows 10 start menu, using Classic Shell click "Start Menu (Windows)" from there you can un-pin the non-existent apps. The option still remains to uninstall for some but does nothing since the apps no longer exist. Another artifact is that suggestions are still enabled. This can be turned off by:

Settings App => Personalization => Start => Occasionally show suggestions in Start

The last artifact are the 3 remaining apps listed in Classic Shell. These can be removed by:

**Classic Shell => All Programs => Apps => Right click => Uninstall
for each**

3.1 Setting Defaults

You will need to set defaults for Firefox and JPEGview. The process for Firefox is:

**Start => Control Panel => Default Programs => Set your default
programs => Firefox => Set this program as default**

The process is the same for Thunderbird as well as anything else you want to have full defaults set. This should mitigate the nagging of windows has with setting your default browser. For JPEGView you will need to set the defaults by following this process:

**Start => Control Panel => Default Programs => Associate a file type
or protocol with a program => select jpeg, nef, png, etc.**

4 Distribution

There are various methods we chose to distribute Windows 10 AME. For convenience, we chose a CloneZilla image, which is the de facto standard cloning and image restoration tool in the FOSS eco-system. This image allows for a clean, error free and reliable imaging of any drive.

We also provide a VHD file, which is a disk-image format directly compatible with virtual machines, skipping any imaging process using CloneZilla. It can however also be imaged to a drive directly.

4.1 How to Write CloneZilla Image

For CloneZilla you will need to put the partclone image onto a seperate drive. In my experience it CloneZilla will not recognize the drive unless it has a bootloader, not sure why, to me that does not seem a very intuitive requirement.

4.1.1 Write CloneZilla to a USB drive

4.1.2 Copy CloneZilla folder and files to a drive

4.1.3 Boot CloneZilla on the target machine with VGA, make sure that the drive with the partclone files is also attached

4.1.4 When you have reached CloneZilla main menu, select "device-image"

4.1.5 Select "local_dev"

4.1.6 Make sure you see the drive with the CloneZilla files before proceeding

4.1.7 Navigate to the folder containing the partclone files, you do not need to select the directory containing the partclone files but instead the folder one level up in the folder structure. Ex.

"/home/test/partclone/ <partclone_files>" if you select "/home/test" CloneZilla will automatically find the image

4.1.8 Select "Beginner"

4.1.9 Select "restoredisk"

4.1.10 Press [Enter] (There should only be one image listed to restore)

4.1.11 Select the target disk

4.1.12 The rest of the options are up to you. After answering the last question (what would you like the machine to do when finished?) it will ask you one last time to confirm, then it will write the image to disk

4.1.13 Reboot into Windows 10 if everything imaged properly

4.2 How to Write a VHD to a Disk

Once you have created your VHD you might look to see if SystemInternals had created a nice GUI for doing something with the VHD besides running it in a virtual machine, they did not. So someone else made their own. Now we have a way to do the reverse of the above step, deploy the VHD to other machines.

4.2.1 Install the target drive into the machine with the VHD image or vice versa

4.2.2 Boot Windows from the source machine's own drive

4.2.3 Download and Run VHD2disk.exe

4.2.4 Select the source VHD you would like to write to the target drive

4.2.5 To find the correct disk number press Start, type diskmgmt.msc, and press enter. There should be a list of disks with the number denoted to them on the left side of the window.

4.3 Expand Partition

Both the CloneZilla image and VHD only produce a partition of about 12GB for the C drive, in order to make Windows use the entire disk, the partition needs to be expanded. So after you have written the image and booted up, run cmd.exe as administrator, run diskpart, list the volumes attached to your machine, select the volume Windows is installed on, and expand.

5 Afterthoughts

When you boot into Windows 10 for the first time after completing this process there are a few things to mention. The total size of removed files is 2GB. You cannot update this Windows installation, ever, even if you try really hard, because it lacks the required components in order to function. As you might have noticed this installation of Windows no longer has any virus protection, as such it is up to you to practice safe computing habits. Again as stated at the beginning, if you really need security, Windows is not the OS to be using, you should be using some form of Linux or BSD. This entire effort was performed by individuals with the aim of making a version of Windows that could be trusted by the user enough that Windows only applications can be used without the fear of information being stolen. We are strong promoters of open source software.