

Cyber Security Survival Kit

Created By: Eric Burdick

Introductions

Hello and thank you for installing The CyberSecurity Survival Kit. This program is your best starting point for anyone who wants to properly defend themselves on the internet. Many other kits and tools are available online and can work very well. However those tools can be seen as overwhelming for anyone not familiar with the more complicated component of the average Windows workstation. On Top of that, it's tough to make a decision of what software to choose, especially when money is involved. The CyberSecurity Survival Kit is built to assist YOU, all of the heavy lifting is all done for you with just little input and work on the customers end. I heavily advise starting with the setup section of the manual as it will ensure that the program is fully operational!

- Eric Burdick

Table of Contents

Introductions.....	2
Table of Contents.....	3
Installation Guide.....	4
Part 1: Github.....	4
Part 2: Powershell Restrictions.....	6
Chapter 1: Start Here!.....	9
Manual.....	9
Stats for Nerds.....	10
Install Choco.....	12
Important!.....	13
Chapter 2: Detection.....	14
Install Malwarebytes.....	14
Microsoft Defender.....	15
Disclaimer.....	16
Install Ublock Origin(Chrome).....	17
Chapter 3: Prevention.....	19
Reboot to Safe Mode.....	19
Search and Destroy.....	21
Turn off Safe Mode.....	22
Chapter 4: Recovery.....	23
Create Restore Point.....	23

Installation Guide

Part 1: Github

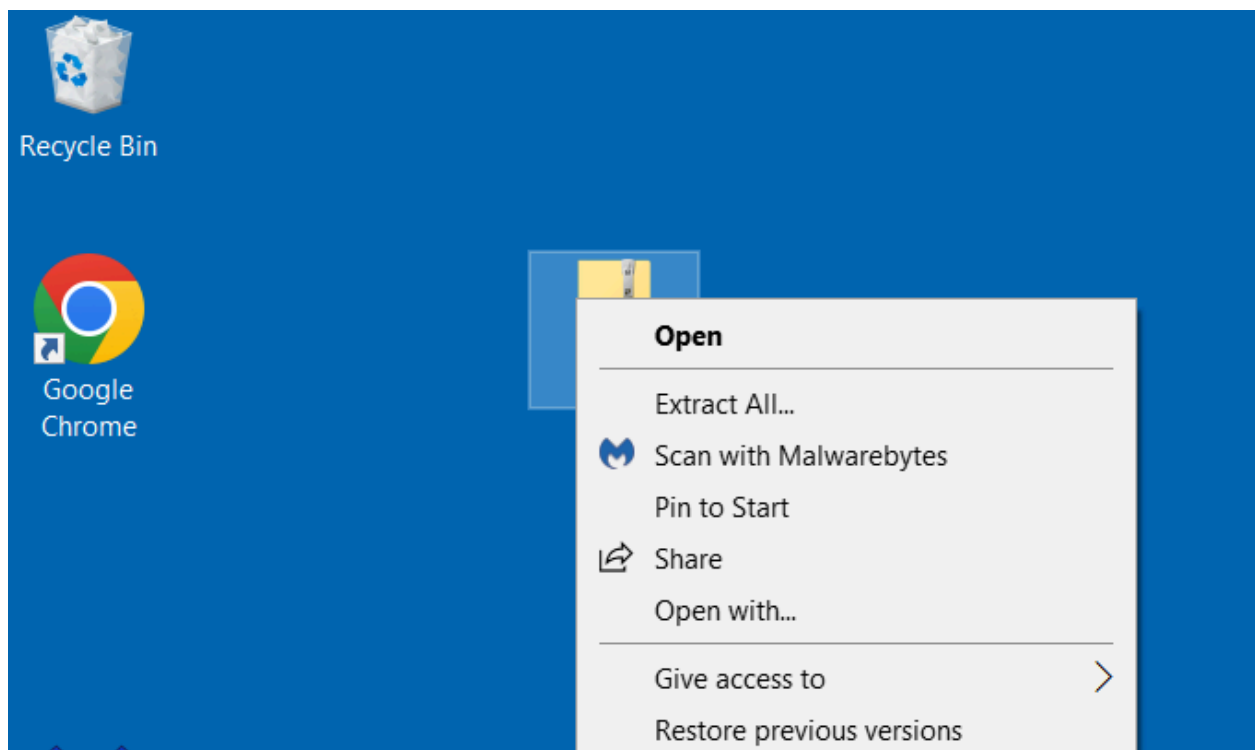
Before starting anything installation wise it's best to verify the current version of the toolkit on the official github webpage. This will allow you to obtain the most up to date version. The toolkit checks the integrity of the files in order to run so if your version of the toolkit is a week outdated **the software will not run and will pop up an error message.**

To begin the installation look for the CSSK.zip folder located on the homepage of the github repository.

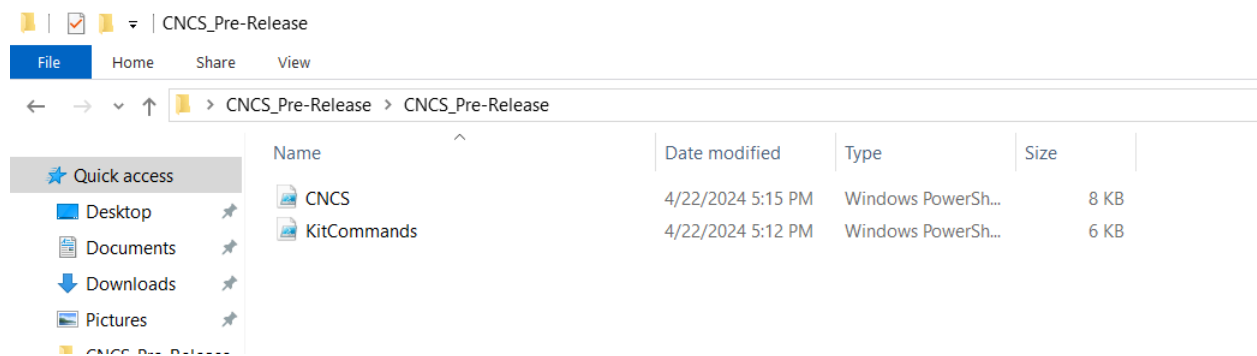


The installation of the folder will begin. Drag or move the folder to your desired location. ZIP files are compressed folders that need to be unzipped. If you already have a file management program(7zip, winrar) then right click on the folder and choose their respective unzip option:

If you do not possess a file management program then place the CSSK.zip into a empty folder:



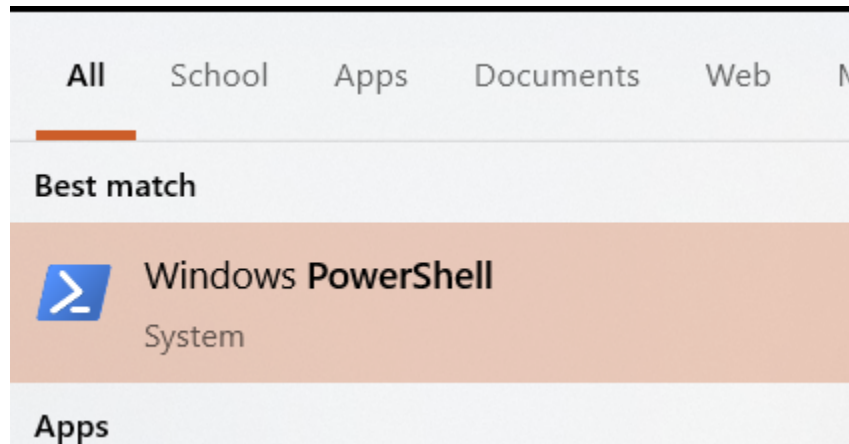
Right click the folder and choose “extract all” this will unpack all the necessary files and a copy of the manual you are reading right now!



Part 2: Powershell Restrictions

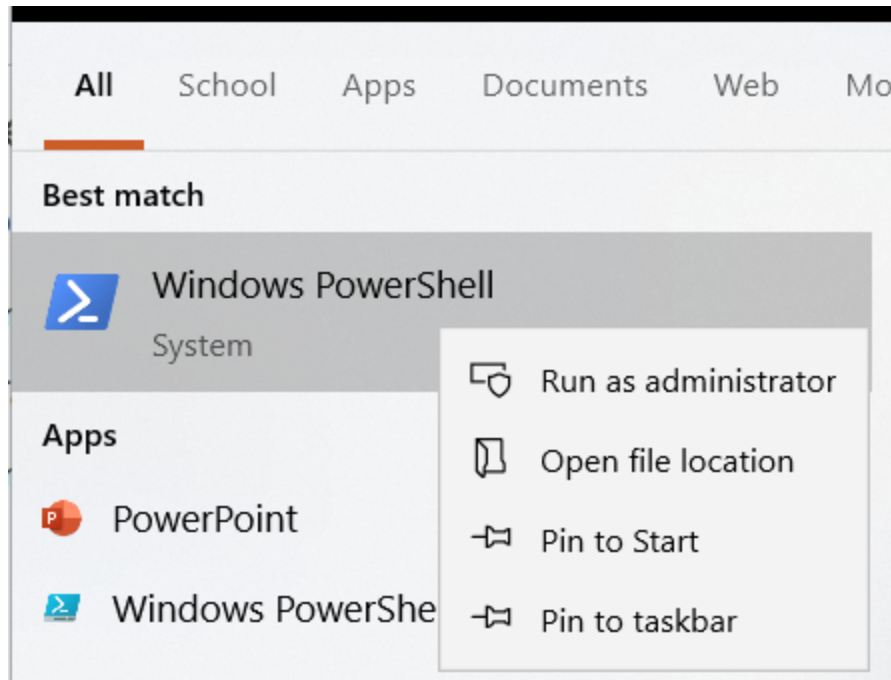
The last thing we need to do is to allow the program to run by altering the Execution-Policy. PowerShell's execution policy is a safety feature that controls the conditions under which PowerShell loads configuration files and runs scripts. This feature helps prevent the execution of malicious scripts. We will temporarily be changing this to allow the program to run but can be set back for maximum security.

To begin open the search bar on Windows:



Type "Powershell" and a program of the same name will pop up.

Right click on the program and select "run as administrator". This allows the program to be run with the most flexibility and versatility especially during installations.



Once a blue window pops up enter the following `Set-ExecutionPolicy AllSigned`

```
PS C:\Users\[redacted] > Set-ExecutionPolicy AllSigned

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"):
```

Once that goes through, you can close the powershell window and start the CyberSecurity Survival Kit.

Opening the program will take a moment but once fully ready to go should display the homepage for the CyberSecurity Survival Kit!

CyberSecurity Survival Kit

Start Here!

Manual

Stats for nerds

Install Chocolatey

Detection

Malwarebytes

Windows Defender

Ublock Origin

Prevention

Reboot to Safe Mode

Search and Destroy

Turn off Safe Mode

Recovery

Create a Backup

Revert to Backup

Chapter 1: Start Here!




For any users who are booting this program up for the first time, welcome! There are some steps that should be consulted first before choosing any other option in the menu as some options require prerequisites before the commands can execute properly.

The others are features that can be referred to at any time for the people wanting to gain a specific understanding of what's going on with the machine in general and instructions.

Manual

Provided within the package is a copy of the manual you are reading right now! The button simply opens the manual for you to read as a pdf document which will open in your default browser. The button is a simple convenience but the file can also be opened within the provided unzipped folder.

It's best to always check for any updates made to the files and manual itself as there may be some changes necessary.

 CNCS	4/22/2024 5:15 PM	Windows PowerSh...	8 KB
 KitCommands	4/22/2024 5:12 PM	Windows PowerSh...	6 KB
 Manual Draft	4/22/2024 6:59 PM	Chrome HTML Do...	1,438 KB

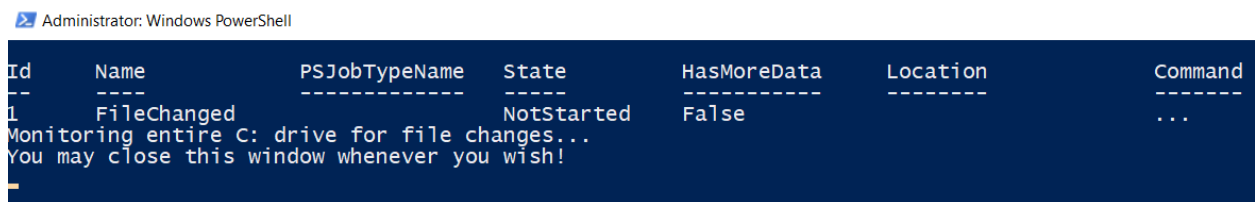
Stats for Nerds

Clicking the “Stats for Nerds” button will open a brand new powershell window with the request to sign into administrator. Depending on your current security settings may for a password

before continuing. This is a great method for maintaining security but for demonstration purposes, the prompt is a simple yes or no:



After clicking yes a new window will pop up:



The following window can stay open or close as much as you wish will listen in on the default (c:) drive of your computer. Any changes made on the file at all will be recorded and recorded within this window.

This is done through Windows EventViewer which allows you to manage and view logs of certain aspects of the system. The provided values describe who, what, where, etc. In a few moments some results should be coming in:

```
Monitoring entire C: drive for file changes...
You may close this window whenever you wish!
File changed: C:\windows\Prefetch\DLLHOST.EXE-766398D2.pf
File changed: C:\windows\Prefetch\DLLHOST.EXE-766398D2.pf
File changed: C:\ProgramData\Malwarebytes\MBAMService\config\UI_IrisSettings.json
File changed: C:\ProgramData\Malwarebytes\MBAMService\config\UI_IrisSettings.json
File changed: C:\ProgramData\Malwarebytes\MBAMService\config\UI_IrisSettings.json
File changed: C:\ProgramData\Malwarebytes\MBAMService\config\UI_IrisSettings.json
File changed: C:\windows\Prefetch\POWERSHELL.EXE-920BBA2A.pf
File changed: C:\windows\Prefetch\POWERSHELL.EXE-920BBA2A.pf
File changed: C:\windows\Prefetch\CONHOST.EXE-1F3E9D7E.pf
File changed: C:\windows\Prefetch\CONHOST.EXE-1F3E9D7E.pf
File changed: C:\Users\champuser\AppData\Local\Temp
File changed: C:\windows\Prefetch\RUNTIMEBROKER.EXE-72C0C855.pf
File changed: C:\windows\Prefetch\RUNTIMEBROKER.EXE-72C0C855.pf
File changed: C:\Users\champuser\AppData\Local\Malwarebytes
File changed: C:\Users\champuser\AppData\Local\Malwarebytes
File changed: C:\Users\champuser\AppData\Local\Malwarebytes\data.db-shm
File changed: C:\Users\champuser\AppData\Local\Malwarebytes\data.db-shm
File changed: C:\Users\champuser\AppData\Local\Malwarebytes
File changed: C:\Windows\ServiceState\EventLog\Data\lastalive0.dat
File changed: C:\Windows\ServiceState\EventLog\Data\lastalive0.dat
File changed: C:\ProgramData\Malwarebytes\MBAMService\config\UI_IrisSettings.json
File changed: C:\ProgramData\Malwarebytes\MBAMService\config\UI_IrisSettings.json
File changed: C:\ProgramData\Malwarebytes\MBAMService\config\UI_IrisSettings.json
File changed: C:\ProgramData\Malwarebytes\MBAMService\config\UI_IrisSettings.json
File changed: C:\windows\ServiceState\EventLog\Data\lastalive1.dat
File changed: C:\windows\ServiceState\EventLog\Data\lastalive1.dat
File changed: C:\ProgramData\Malwarebytes\MBAMService\config\UI_IrisSettings.json
File changed: C:\ProgramData\Malwarebytes\MBAMService\config\UI_IrisSettings.json
File changed: C:\ProgramData\Malwarebytes\MBAMService\config\UI_IrisSettings.json
File changed: C:\ProgramData\Malwarebytes\MBAMService\config\UI_IrisSettings.json
File changed: C:\ProgramData\Malwarebytes\MBAMService\config\UI_IrisSettings.json
File changed: C:\Windows\ServiceState\EventLog\Data\lastalive0.dat
```

It's best to use this only if you want to see what's going on under the hood. Because this monitors a whole drive, many results will be coming in at the same time.

Install Choco

Clicking this option will open a brand new powershell window(refer to page #) where the installation will begin.

The installer is called Chocolatey, a package manager which can install a vast library of software and programs through the use of the command line. However the use of Chocolatey within this toolkit is so that the command aspect of the installs are done for you.

This will take some time so please do not close out of the window until the installation is finished.

```
Administrator: Windows PowerShell
Forcing web requests to allow TLS v1.2 (Required for requests to Chocolatey.org)
Getting latest version of the Chocolatey package for download.
Not using proxy.
Getting Chocolatey from https://community.chocolatey.org/api/v2/package/chocolatey/2.2.2.
Downloading https://community.chocolatey.org/api/v2/package/chocolatey/2.2.2 to C:\Users\CHAMPU~1\AppData\Local\Temp\cho
colatey\chocoInstall\chocolatey.zip
Not using proxy.
Extracting C:\Users\CHAMPU~1\AppData\Local\Temp\chocolatey\chocoInstall\chocolatey.zip to C:\Users\CHAMPU~1\AppData\Loca
l\Temp\chocolatey\chocoInstall
Installing Chocolatey on the local machine
```

```
Creating ChocolateyInstall as an environment variable (targeting 'Machine')
Setting ChocolateyInstall to 'C:\ProgramData\chocolatey'
WARNING: It's very likely you will need to close and reopen your shell
before you can use choco.
Restricting write permissions to Administrators
We are setting up the Chocolatey package repository.
The packages themselves go to 'C:\ProgramData\chocolatey\lib'
(i.e. C:\ProgramData\chocolatey\lib\yourPackageName).
A shim file for the command line goes to 'C:\ProgramData\chocolatey\bin'
and points to an executable in 'C:\ProgramData\chocolatey\lib\yourPackageName'.

Creating Chocolatey folders if they do not already exist.

chocolatey.nupkg file not installed in lib.
Attempting to locate it from bootstrapper.
PATH environment variable does not have C:\ProgramData\chocolatey\bin in it. Adding...
WARNING: Not setting tab completion: Profile file does not exist at
'C:\Users\champuser\Documents\WindowsPowerShell\Microsoft.PowerShell_profile.ps1'.
Chocolatey (choco.exe) is now ready.
You can call choco from anywhere, command line or powershell by typing choco.
Run choco /? for a list of functions.
You may need to shut down and restart powershell and/or consoles
first prior to using choco.
Ensuring Chocolatey commands are on the path
Ensuring chocolatey.nupkg is in the lib folder
```

Once finished you can fully close the window. Chocolatey will be called for a few of the features later in this manual.

Important!

You may get a popup saying that "" has been installed but requires a reboot. To do this, simply restart your computer. After the reboot, choose to install chocolatey again and the install should run smoothly.

```
.NET Framework 4.8 was installed, but a reboot is required.  
Please reboot the system and try to install/upgrade Chocolatey again.  
At C:\Users\champuser\AppData\Local\Temp\chocolatey\chocoInstall\tools\chocolateysetup.psm1:815 char:11  
+ throw ".NET Framework 4.8 was installed, but a reboot is re ...  
+ ~~~~~  
+ CategoryInfo          : OperationStopped: (C:\NET Framework ...ocolatey again.:String) [], RuntimeException  
+ FullyQualifiedErrorId : .NET Framework 4.8 was installed, but a reboot is required.  
Please reboot the system and try to install/upgrade Chocolatey again.
```

Chapter 2: Detection

These are the options for people who seek assistance in detecting and alerting the user in the case of malicious activity and programs. The buttons provided install the programs for you. This is because it can be tricky to find the proper programs to install especially now that fake websites can exist out there.

Install Malwarebytes

Disclaimer! Please ensure Chocolatey is installed before choosing this option!

This is the first program that utilizes Chocolatey for installs. All you need to do is press the button. The program will check to see if Chocolatey is installed, you will get an error if it is not detected on your system!

```
Administrator: Windows PowerShell
Installing Malwarebytes...
chocolatey v2.2.2
Installing the following packages:
malwarebytes
By installing, you accept licenses for the packages.
Progress: Downloading malwarebytes 5.1.2.88... 100%

malwarebytes v5.1.2.88 [Approved]
malwarebytes package files install completed. Performing other installation steps.
Downloading malwarebytes
  from 'https://downloads.malwarebytes.com/file/mb-windows'
Progress: 100% - Completed download of C:\Users\champuser\AppData\Local\Temp\chocolatey\malwarebytes\5.1.2.88\MBSetup.exe (2.47 MB).
Download of MBSetup.exe (2.47 MB) completed.
Hashes match.
Installing malwarebytes...
malwarebytes has been installed.
malwarebytes may be able to be automatically uninstalled.
The install of malwarebytes was successful.
Software installed to 'C:\Program Files\Malwarebytes\Anti-Malware'

Chocolatey installed 1/1 packages.
See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).

Enjoy using Chocolatey? Explore more amazing features to take your
experience to the next level at
https://chocolatey.org/compare
Malwarebytes has been installed!
```


Malwarebytes should now appear on your desktop as a shortcut icon. You can open that up and run the script as much as you please. The program will check for updates whenever you like!

- Dashboard
- Settings


SECURITY


 **Scanner** Start your first scan Scan ⋮

 **Detection History** ⋮

 **Real-Time Protection** Active ⋮

ONLINE PRIVACY

 **VPN** Premium Plus Your connection is Public ☐ OFF ⋮

 **Stockholm** Change



Private IP: Not connected

TRUSTED ADVISOR

This PC View details



Scan this device to view your protection status.

Other devices Refresh

Enjoy the convenience of protecting multiple devices with one subscription.

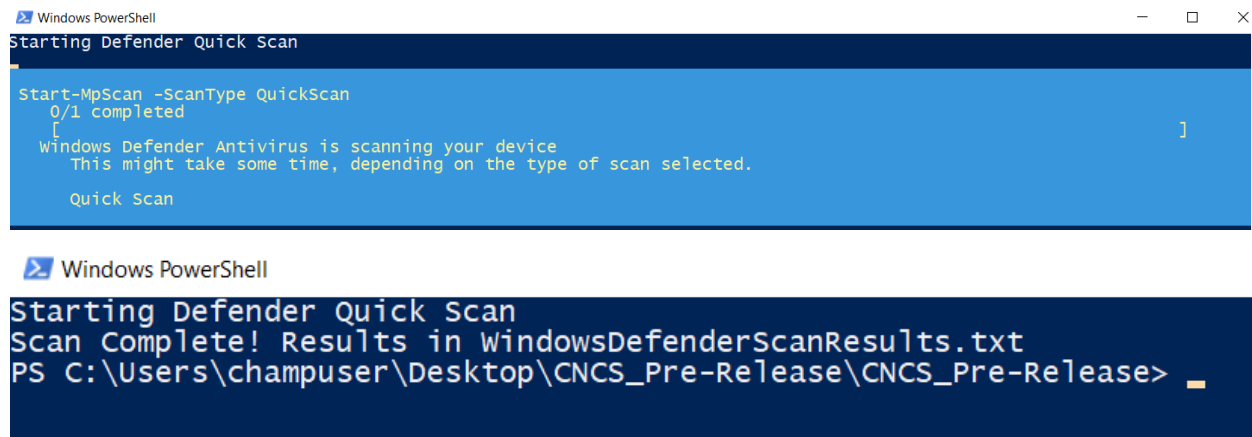


[See protection plans](#)

Microsoft Defender

Microsoft Defender is the built in antivirus scanner for Windows machines. It comes with a variety of scans that are able to scan, identify and delete!

While the program can be accessed whenever you want by searching for the program. The Cyber Security Survival Kit has a built-in quick scan using Defender.






```
Windows PowerShell
Starting Defender Quick Scan

Start-MpScan -ScanType QuickScan
0/1 completed
[
  Windows Defender Antivirus is scanning your device.
  This might take some time, depending on the type of scan selected.
  Quick Scan
]

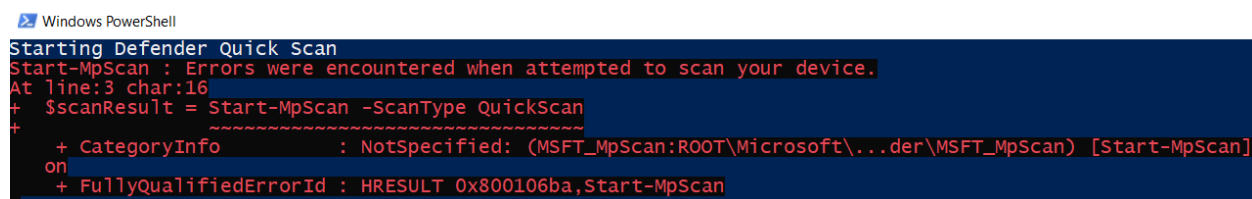
Windows PowerShell
Starting Defender Quick Scan
Scan Complete! Results in WindowsDefenderScanResults.txt
PS C:\Users\champuser\Desktop\CNCS_Pre-Release\CNCS_Pre-Release>
```

A text document called **WindowsDefenderScanResults.txt** should appear within your program folder. If the page is blank then the defender found nothing on your system it deems malicious.

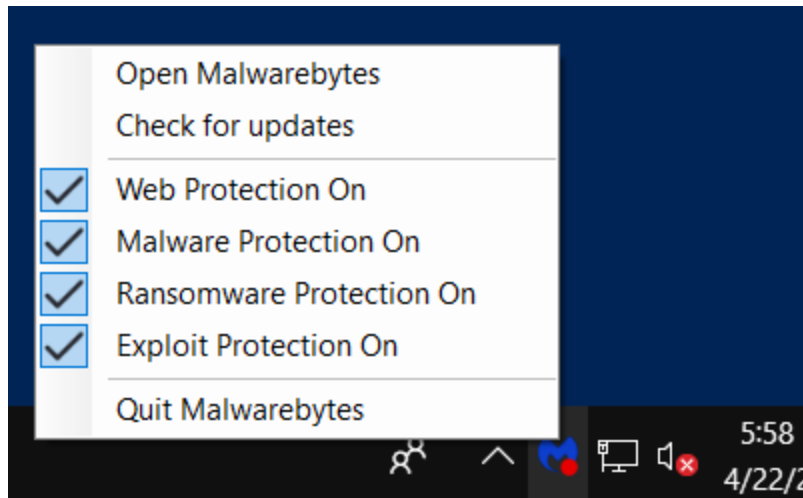
Name	Date modified	Type	Size
 CNCS	4/22/2024 5:15 PM	Windows PowerSh...	8 KB
 KitCommands	4/22/2024 5:12 PM	Windows PowerSh...	6 KB
 WindowsDefenderScanResults	4/22/2024 5:53 PM	Text Document	0 KB

Disclaimer

If you have installed Malwarebytes or any other antivirus of your choice. You may get an error. Windows Defender actually takes a step back when it detects another antivirus on your system. If you still wish to run this scan you can simply turn off the program in the right corner of your desktop.



```
Windows PowerShell
Starting Defender Quick Scan
Start-MpScan : Errors were encountered when attempted to scan your device.
At line:3 char:16
+ $scanResult = Start-MpScan -ScanType QuickScan
+ ~~~~~
+ CategoryInfo          : NotSpecified: (MSFT_MpScan:ROOT\Microsoft\...der\MSFT_MpScan) [Start-MpScan]
+ FullyQualifiedErrorId : HRESULT 0x800106ba,Start-MpScan
```

Install Ublock Origin(Chrome)

Disclaimer! Please ensure Chocolatey is installed before choosing this option!

Ublock Origin is a popular extension for Google Chrome. This blocks websites it detects as malicious. This also blocks all ads on websites, this is because ads can be seen as malicious and masquerade as a legitimate website. The install functions through Chocolatey so the install is done for you!

```
Administrator: Windows PowerShell
Installing uBlock Origin for Chrome...
chocolatey v2.2.2
Installing the following packages:
ublockorigin-chrome
By installing, you accept licenses for the packages.
Progress: Downloading chocolatey-compatibility.extension 1.0.0... 100%
chocolatey-compatibility.extension v1.0.0 [Approved]
chocolatey-compatibility.extension package files install completed. Performing other installation steps.
Installed/updated chocolatey-compatibility extensions.
The install of chocolatey-compatibility.extension was successful.
Software installed to 'C:\ProgramData\chocolatey\extensions\chocolatey-compatibility'
Progress: Downloading chocolatey-core.extension 1.4.0... 100%
chocolatey-core.extension v1.4.0 [Approved]
chocolatey-core.extension package files install completed. Performing other installation steps.
Installed/updated chocolatey-core extensions.
The install of chocolatey-core.extension was successful.
Software installed to 'C:\ProgramData\chocolatey\extensions\chocolatey-core'
Progress: Downloading GoogleChrome 124.0.6367.60... 100%
GoogleChrome v124.0.6367.60 [Approved]
GoogleChrome package files install completed. Performing other installation steps.
WARNING: Unable to find the architecture of the installed Google Chrome application
Downloading googlechrome 64 bit
from 'https://dl.google.com/dl/chrome/install/googlechromestandaloneenterprise64.msi'
Progress: 100% - Completed download of C:\Users\champuser\AppData\Local\Temp\chocolatey\GoogleChrome\124.0.6367.60\goog
chromestandaloneenterprise64.msi (109.91 MB).
Download of googlechromestandaloneenterprise64.msi (109.91 MB) completed.
Error - hashes do not match. Actual value was '480EC825C78A7C7310FB4F2CC83AB8B57F258827DF0EC5AEB8E63956C7A31398'.
```

Google Chrome is actually included within the package so if you already have the browser installed then an error will pop. This can be ignored.

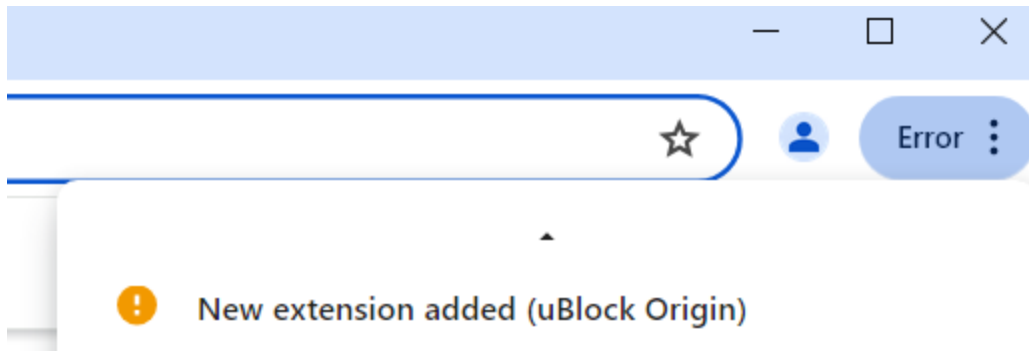
```
ublockorigin-chrome v1.19.6 [Approved]
ublockorigin-chrome package files install completed. Performing other installation steps.
The install of ublockorigin-chrome was successful.
Software install location not explicitly set, it could be in package or
default install location of installer.

Chocolatey installed 3/4 packages. 1 packages failed.
See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).

Failures
- GoogleChrome (exited -1) - Error while running 'C:\ProgramData\chocolatey\lib\GoogleChrome\tools\chocolateyInstall.
1'.
See log for details.
uBlock Origin has been installed!
PS C:\Windows\system32
```

This button only works for users who use Google Chrome so ignore this button if you have another browser of choice! Blockers are important and should be researched for your browser of choice!

Next time you open chrome you will see a prompt:



"uBlock Origin" added

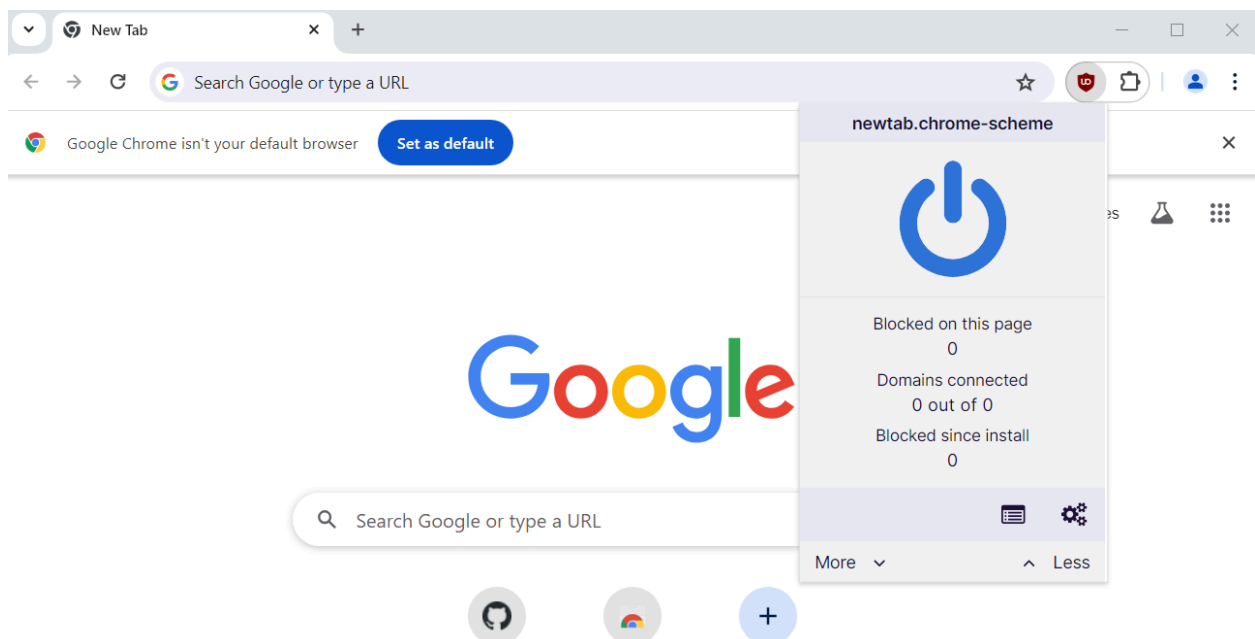
Another program on your computer added an extension that may change the way Chrome works.

It can:

- Read and change all your data on all websites
- Change your privacy-related settings

Enable extension

Remove from Chrome



Chapter 3: Prevention

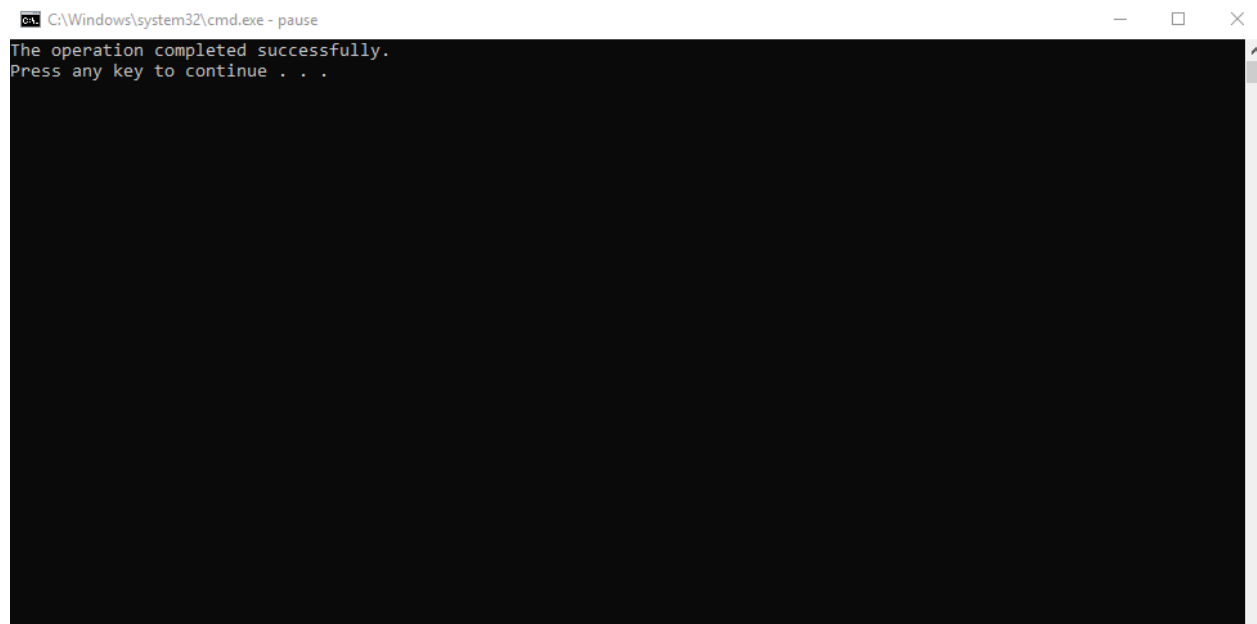
The following options are for people who believe they do have a form of virus on your machine. These tools are for people who wish to upgrade their tools in removal of the software. However it's important to note that Malwarebytes and Defender do have their own removal options so consider those options as well.

Reboot to Safe Mode

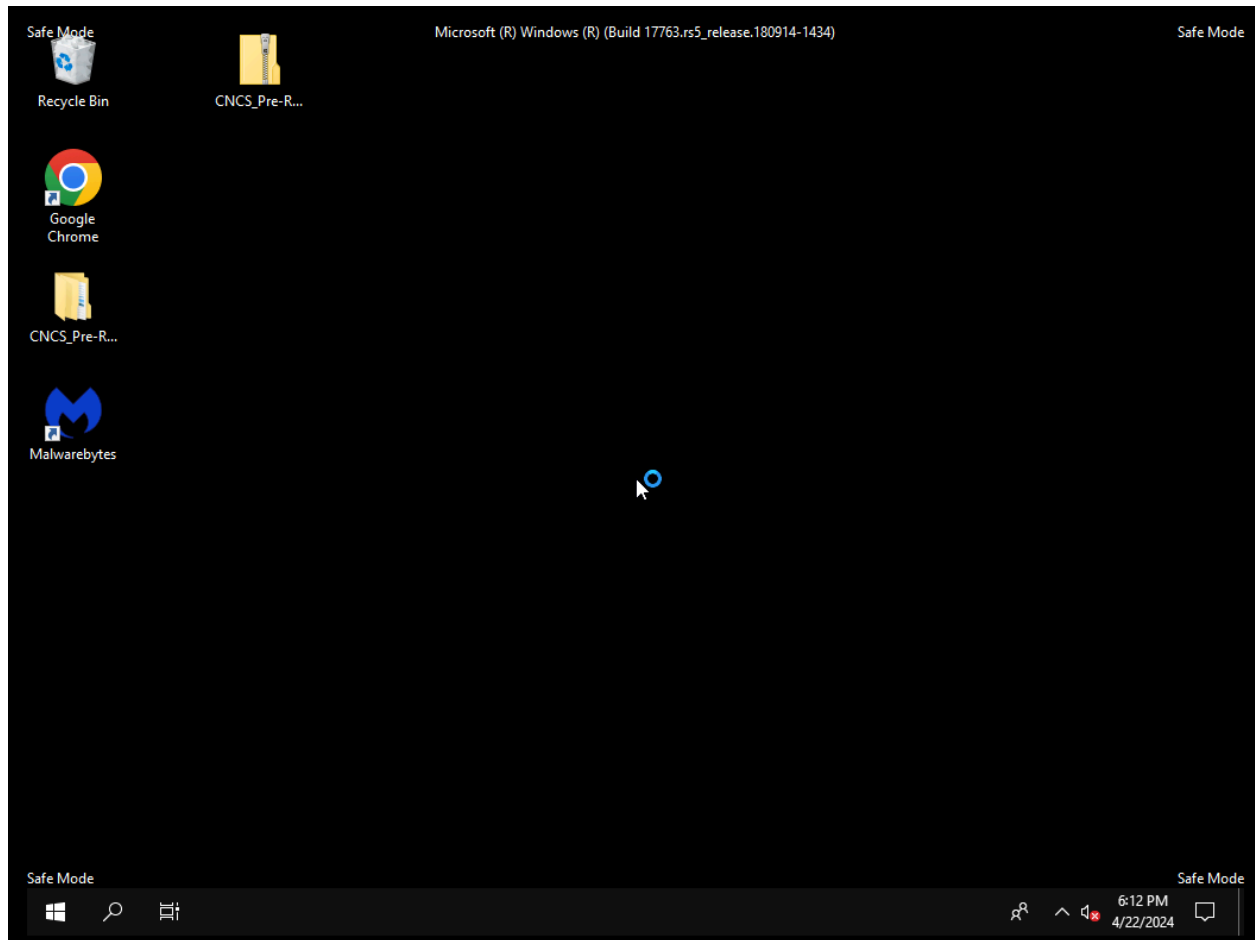
This action should be taken last after everything has been installed.

Safe mode is a toggle within the Windows OS that puts the computer into a limited state cutting off internet access, drivers and other normal functions. This is a measure that should be taken if you already believe you have a virus on a computer and cannot be removed. This is because some viruses require internet access to function, so safe mode can cut off the roots of the problem.

Selecting the button will open the command prompt instead, this is normal as the command to switch to safe mode only works here. The window will only say the command has been done.

A screenshot of a Windows Command Prompt window. The title bar at the top reads "C:\Windows\system32\cmd.exe - pause". The main area of the window is black with white text. The text displayed is "The operation completed successfully." followed by "Press any key to continue . . .". The window has standard Windows window controls (minimize, maximize, close) in the top right corner.

You will need to restart your machine for this to take effect. Upon reboot and login, you should see something like this:



Internet access has been turned off so in order to disable this please go to powershell and enter the following after your scans have been done:

Unset

```
Start-Process cmd.exe -Verb RunAs -ArgumentList "/k bcdedit /deletevalue  
{default} safeboot & pause" -ErrorAction SilentlyContinue
```

Restarting the computer will put the computer back into a non safe mode!

Search and Destroy

This option installed the Emsisoft Emergency Kit. A much more advanced antivirus that will remove any malicious files off your computer. This is the third and final install through Chocolatey. The install should look like this.

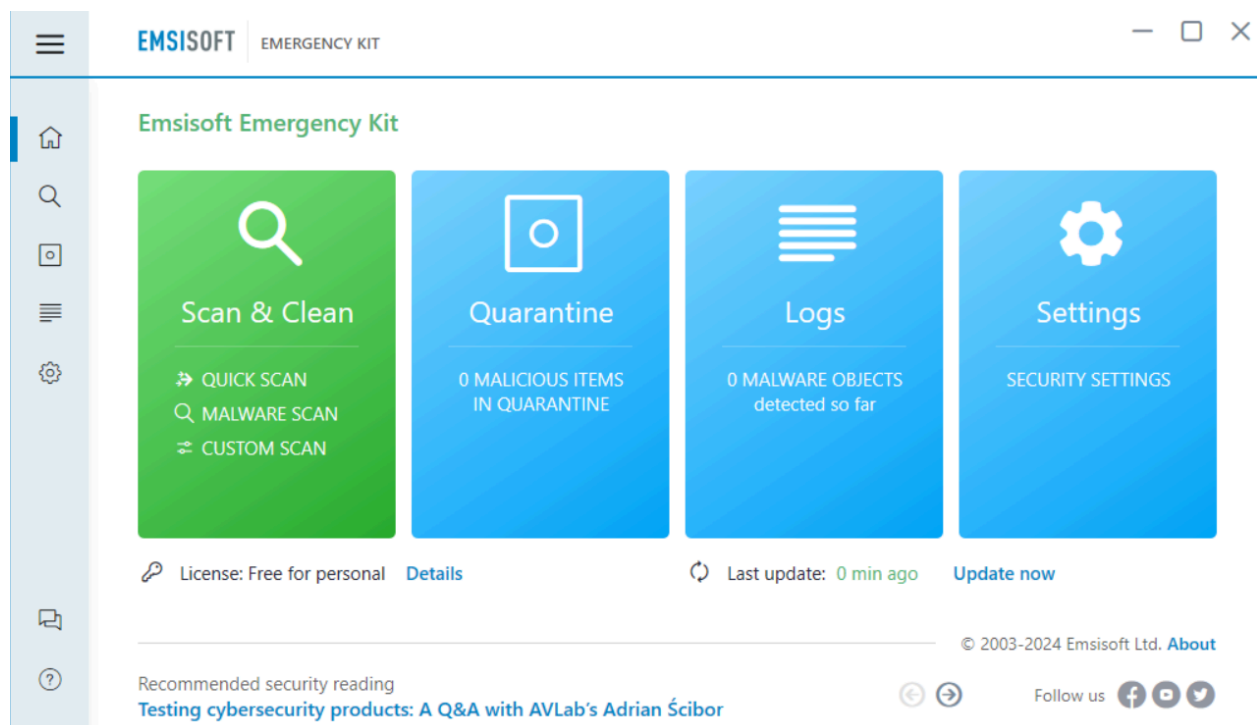
```
Administrator: Windows PowerShell
Installing Emsisoft Emergency Kit...
chocolatey v2.2.2
Installing the following packages:
emsisoft-emergency-kit
By installing, you accept licenses for the packages.
Progress: Downloading emsisoft-emergency-kit 2024.4.0.12347... 100%

emsisoft-emergency-kit v2024.4.0.12347 [Approved]
emsisoft-emergency-kit package files install completed. Performing other installation steps.
The package emsisoft-emergency-kit wants to run 'chocolateyInstall.ps1'.
Note: If you don't run this script, the installation will fail.
Note: To confirm automatically next time, use '-y' or consider:
choco feature enable -n allowGlobalConfirmation
Do you want to run the script?([Y]es/[A]ll - yes to all/[N]o/[P]rint): A

Downloading emsisoft-emergency-kit
from 'https://dl.emsisoft.com/EmsisoftEmergencyKit.exe'
Progress: 100% - Completed download of C:\Users\champuser\AppData\Local\Temp\chocolatey\emsisoft-emergency-kit\2024.4.12347\EmsisoftEmergencyKit.exe (353.54 MB).
Download of EmsisoftEmergencyKit.exe (353.54 MB) completed.
WARNING: Ignoring checksums due to feature checksumFiles turned off or option --ignore-checksums set.
Installing emsisoft-emergency-kit...
emsisoft-emergency-kit has been installed.
The install of emsisoft-emergency-kit was successful.
Software installed as 'EXE', install location is likely default.

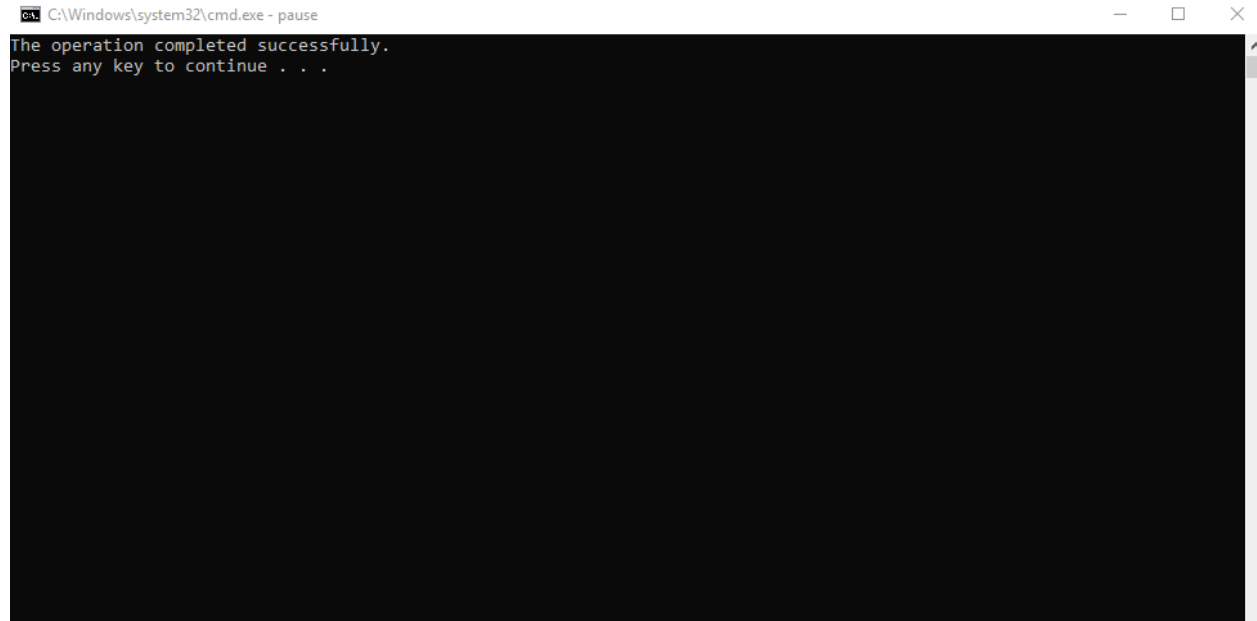
Chocolatey installed 1/1 packages.
See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).
Emsisoft Emergency Kit has been installed!
PS C:\Windows\system32>
```

Right away Emsisoft will get to work and pop up right away!



Turn off Safe Mode

This option is for those who accidentally clicked the **Reboot to Safe Mode** button by accident or changed their mind regarding safe mode. Choosing this option will similarly open the cmd and pop the following message:



```
C:\Windows\system32\cmd.exe - pause
The operation completed successfully.
Press any key to continue . . .
```



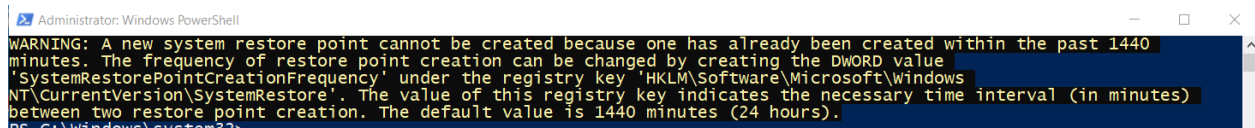
Chapter 4: Recovery

This option is all about preparing for the worst! The case where your computer becomes completely taken over or files have been encrypted. This option mainly works through restore points to revert to a stable and previous version of your machine. This should be done every now and then to reduce overall data loss.

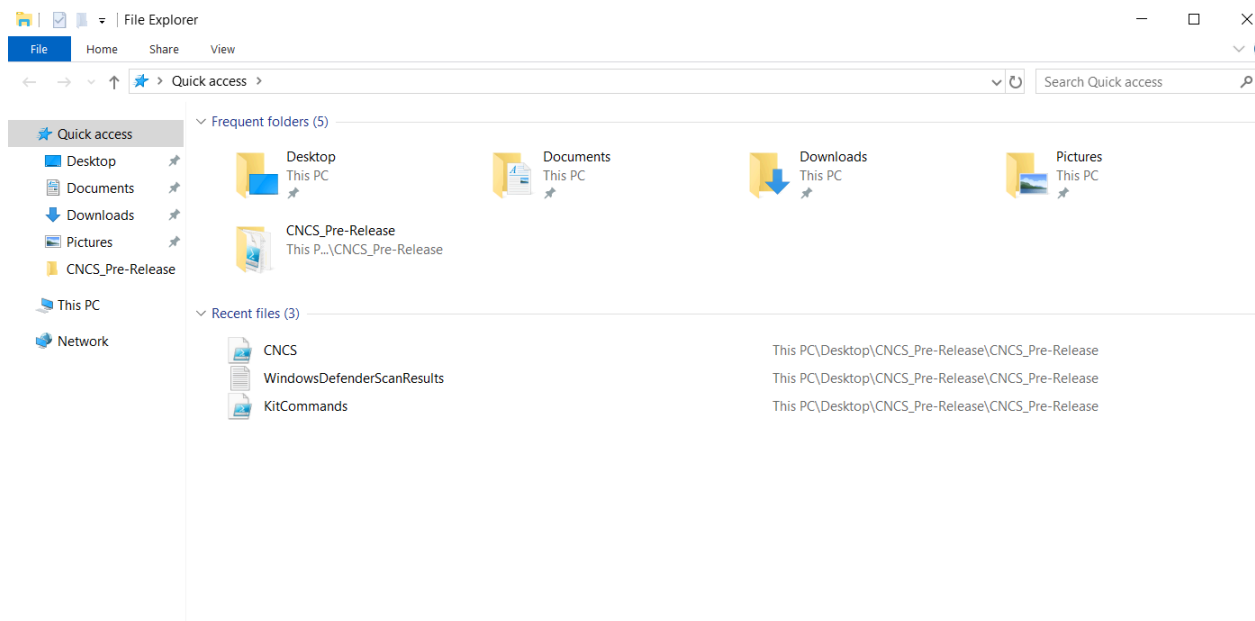
Create Restore Point

This option creates the restore point necessary as a backup. This will take a few minutes but once completed will show an empty command prompt when finished.

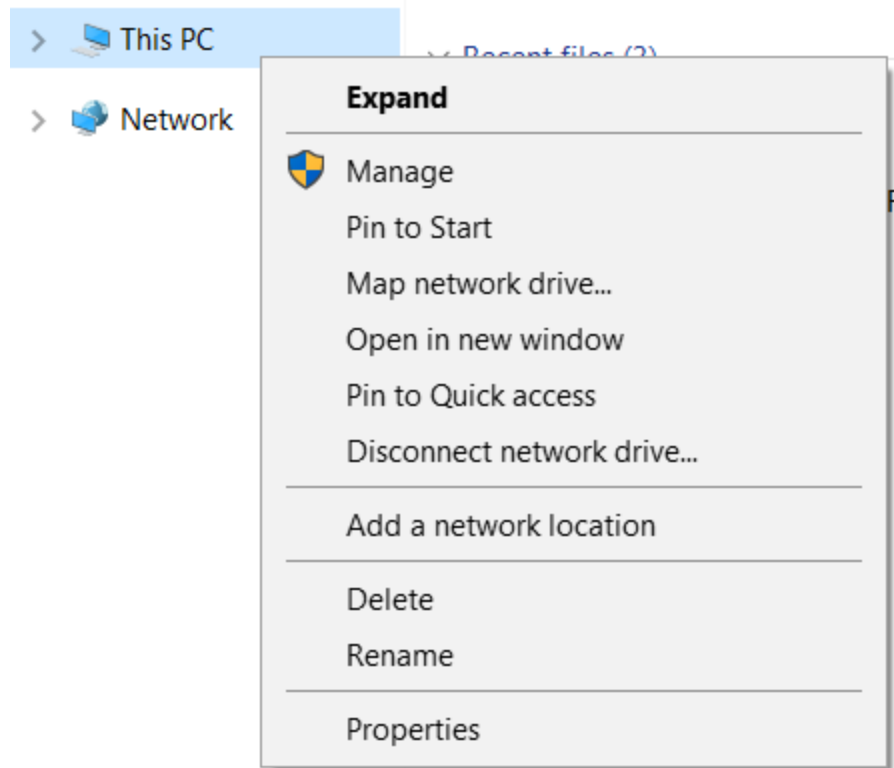
If run again you will receive this screen starting to wait between restore points.



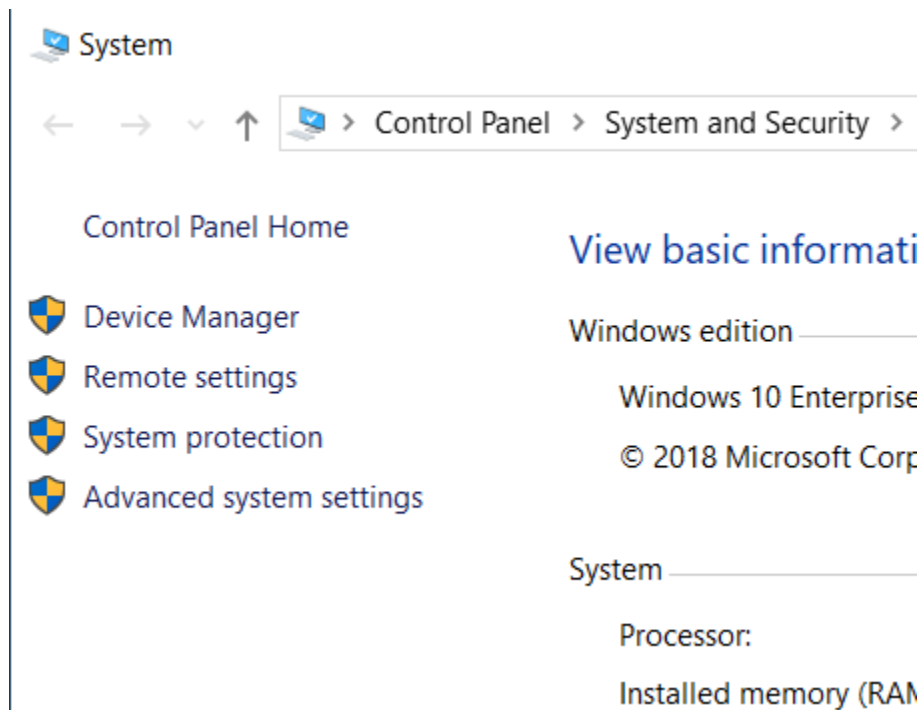
If you get another error please verify your machines allow restore points by searching and opening File Explorer.



Right click This PC and select Properties:



Select System Protection:



If the option is blanked out please consult your administrator as it may be disabled for security purposes. If not then select create.

Protection Settings

Available Drives	Protection
 Local Disk (C:) (System)	On

Configure restore settings, manage disk space, and delete restore points.

Configure...

Create a restore point right now for the drives that have system protection turned on.

Create...

You will be asked to dedicate space for your backup. Please select the amount of space you are willing to use for backups.

System Protection



Create a restore point

Type a description to help you identify the restore point. The current date and time are added automatically.

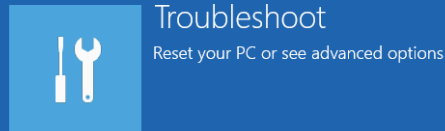
CSSK_Backup

Create

Cancel

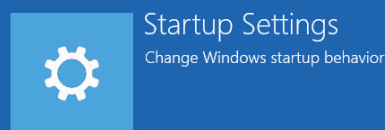
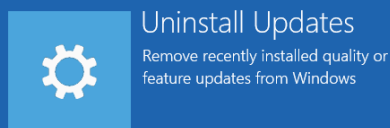
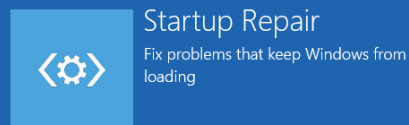
To use a restore point hold shift and restart your computer. You will be met with this screen:

Choose an option



Choose Troubleshoot > Advanced Options > System Restore

← Advanced options



Your PC will now be reverted back to the restore point. It will be the exact same when it was created. If you created multiple restore points then you can select the one of choice. CSSK is our manual one while Test is the Survival Kits backup.

