

Forum:[Hack Forums](#)

Thread: [Hiding Drives Using The Registry](#)

WeedIsInTheAir - September 23, 2022, 3:42 pm

Disclaimer >> You can find the original project and/or source in codeproject under the creator's name Gun Gun Febrianza.

Perfect for beginners.

Useful to some, useless to others.

The creator left us a little message about the program:

Gun Gun Febrianza Wrote:We must create a subkey in HKEY_CURRENT_USER and this is the path Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer we must create DWORD 'NoDrives' with value 4. Value 4 is used for hiding drive 'C'.

Straight to the point. But not giving a lot of info either.

We can Google ss64/nt/syntax-nodrives and learn more about this.

SS64 Wrote:Copy the result into the registry to hide the drive letter(s)

User Key:

[HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer]

System Key:

[HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer]

Value Name: NoDrives

Data Type: DWORD

After changing the registry, logoff or reboot so that it takes effect.

This entry stores the setting of the 'Hide these specified drives' in My Computer Group Policy. Group Policy adds this entry to the registry when you enable the policy. If you disable the policy or set it to Not configured, Group Policy deletes this entry from the registry, and the system behaves as though the value is 0x0.

Drive mappings hidden with a nodrives registry setting are still available, just type the drive letter into the Windows explorer address bar.

And even a deep quote by Carl Jung?

Quote:"The dream is the small hidden door in the deepest and most intimate sanctum of the soul, which opens to that primeval cosmic night that was soul long before there was conscious ego and will be soul far beyond what a conscious ego could ever reach" ~ Carl Jung

Now that we know what we're doing, let's peek the code.

First thing we encounter is a restart() function

Code private void restart()

```
{  
    Process p = new Process();
```

```

foreach (System.Diagnostics.Process exe in System.Diagnostics.Process.GetProcesses())
{
    if (exe.ProcessName == "explorer")
        exe.Kill();
}

```

After hiding our drive(s) we are required to logoff/reboot in order to see the changes. This function kills the process explorer.exe (which is charge of displaying the UI) and runs it again. This allows us to see the changes without rebooting or logging off.

Terminating the process via Task Manager will force you to start a new task as it won't start by itself. Just in case someone wondered.

Let's continue exploring the *magic* behind scenes

Code private void button_HideDrive_click(object sender, EventArgs e)

```

{
    try
    {
        if (comboBox1.SelectedItem.ToString() == "C")
        {
            string noDrive = "Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer";
            RegistryKey regKey = Registry.CurrentUser.CreateSubKey(noDrive);

            regKey.SetValue("NoDrives", Convert.ToInt32("4", 16), RegistryValueKind.DWord);
            regKey.Close();
            MessageBox.Show("Drive hidden successfully");

            restart();
        }
    }
    catch
    {
        MessageBox.Show("Something went wrong\n Try running with admin privileges");
    }
}

```

As we already know what we are doing, this function is pretty self explanatory. Creating a registry key with the values "NoDrives" and value 4.

Why 4? It's the value needed in order to hide the C: drive.

More info can be found at the original project, you can click below to see other values.

Spoiler ([Click to View](#))

Value 4 using for hide drive = C

Value 8 using for hide drive = D

Value 10 using for hide drive = E

Value 20 using for hide drive = F

Value 40 using for hide drive = G

Value 80 using for hide drive = H

Value 100 using for hide drive = I

Value 200 using for hide drive = J

Value 400 using for hide drive = K

Value 800 using for hide drive = L

Value 1000 using for hide drive = M

Value 2000 using for hide drive = N
Value 4000 using for hide drive = O
Value 8000 using for hide drive = P
Value 10000 using for hide drive = Q
Value 20000 using for hide drive = R
Value 40000 using for hide drive = S
Value 80000 using for hide drive = T
Value 100000 using for hide drive = U
Value 200000 using for hide drive = V
Value 400000 using for hide drive = W
Value 800000 using for hide drive = Y
Value 1000000 using for hide drive = X
Value 2000000 using for hide drive = Z
Value 3ffffff used for hide = All Drive

Finally we close the registry and invoke the restart() function we talked about before, allowing us to see the changes in our system.

I don't need to explain that this doesn't protect/encrypt your drive(s), right?

Regards,