

Forum:[Hack Forums](#)

Thread: [Efficient ways to drop exe to specific directory](#)

JoseCmanXDII - January 14, 2022, 2:50 pm

so i was looking for ways that if a victim run my exe it creates itself to other different directory (without destroying the actual exe of of course because that will be suspicious) so i can after add it easily to startup

i found this method but its detected by antivirus i tested (kaspersky) At Runtime!

Code using (FileStream fileStream = new FileStream(path, FileMode.Create, FileAccess.Write))

```
{
    byte[] Buffer1 = File.ReadAllBytes(Application.ExecutablePath);
    fileStream.Write(x1, 0, x1.Length);
    byte[] Buffer2 = new byte[(Any Number)];
    fileStream.Write(f2, 0, f2.Length);
}
```

}i would like to know any other alternative ways.. im sorry im still learning basics im not good if their is more simple way to this i would like to know

itcorp - January 14, 2022, 4:36 pm

(Jan 14, 2022 03:50 PM)JoseCmanXDII Wrote: [\[CITE\]](#) so i was looking for ways that if a victim run my exe it creates itself to other different directory (without destroying the actual exe of of course because that will be suspicious) so i can after add it easily to startup

i found this method but its detected by antivirus i tested (kaspersky) At Runtime!

Code using (FileStream fileStream = new FileStream(path, FileMode.Create, FileAccess.Write))

```
{
    byte[] Buffer1 = File.ReadAllBytes(Application.ExecutablePath);
    fileStream.Write(x1, 0, x1.Length);
    byte[] Buffer2 = new byte[(Any Number)];
    fileStream.Write(f2, 0, f2.Length);
}
```

}i would like to know any other alternative ways.. im sorry im still learning basics im not good if their is more simple way to this i would like to know

The very idea of a dropper is that has been designed to install some sort of malware to a target system. The malware code can be contained within the dropper and such droppers are considered as single-stage dropper and that is achieved in various ways such as hard coding,codedom etc...But if you are in an attempt to avoid detection by av it may contains the ability to download malware with exec which downloads the malware and then activates it and such droppers are called two-stage droppers which is nowadays manifested through exploits which can be written in various programming languages whether they are abusing the programming language itself or some popular software like word.excel,powerpoint,pdf reader etc...This forum already has great examples so I advise you to take your time and take a look forum a bit, a similar question was recently asked here <https://hackforums.net/showthread.php?tid=6186678>.

Perseverance and creativity are important in designing things like this,I think I have provided you with enough information to get you started, because the sky is your limit.I wish you all the best and continue with hard work bud.

JoseCmanXDII - January 14, 2022, 9:12 pm

(Jan 14, 2022 05:36 PM)itcorp Wrote: [\[CITE\]](#) The very idea of a dropper is that has been designed to install some sort of malware to a target system. The malware code can be contained within the dropper and such droppers are considered as single-stage dropper and that is achieved in various ways such as hard coding, codedom etc... But if you are in an attempt to avoid detection by av it may contains the ability to download malware with exec which downloads the malware and then activates it and such droppers are called two-stage droppers which is nowadays manifested through exploits which can be written in various programming languages whether they are abusing the programming language itself or some popular software like word.excel,powerpoint,pdf reader etc... This forum already has great examples so I advise you to take your time and take a look forum a bit, a similar question was recently asked here <https://hackforums.net/showthread.php?tid=6186678>.

Perseverance and creativity are important in designing things like this, I think I have provided you with enough information to get you started, because the sky is your limit. I wish you all the best and continue with hard work bud.

thanks for your reply but i think you are over complicating it. my malware is just a clipboard changer so i dont want all of this cuz i wont use either dropper or downloader and i dont use any type of https or sockets im just into the more simple ways which are far away from antivirus suspicious behavior

jmark7 - January 15, 2022, 1:58 am

You can use `System.IO.File.WriteAllBytes(path, bytes);` to perform this action.

0x9F - January 17, 2022, 1:09 am

(Jan 14, 2022 10:12 PM)JoseCmanXDII Wrote: [\[CITE\]](#) thanks for your reply but i think you are over complicating it. my malware is just a clipboard changer so i dont want all of this cuz i wont use either dropper or downloader and i dont use any type of https or sockets im just into the more simple ways which are far away from antivirus suspicious behavior

You are not far away from any other malware when you call it yourself "malware". If you want to keep it simple, you will get dicked on by AV engines in scan/runtime. If your actions weren't any suspicious, a proper AV engine wouldn't flag it in the first line. Deal with it.

goodrabbit - March 3, 2022, 3:56 am

Would recommend you:
using `System.IO;`

```
File.Move("dirOld","dirNew")
```

JoseCmanXDII - March 5, 2022, 8:12 pm

(Mar 3, 2022 04:56 AM)goodrabbit Wrote: [\[CITE\]](#) Would recommend you:
using `System.IO;`

```
File.Move("dirOld","dirNew")
```

oh how i didn't think of that. thanks!

World - March 6, 2022, 1:21 pm

If you're melting the exe, I'd recommend using cmd to copy

Trigger Warning: Ghetto code
`Code Process.Start("cmd.exe", $"/c copy '{System.Reflection.Assembly.GetEntryAssembly().Location}' 'c:/droplocation/my.exe'");`
Can't guarantee it would bypass Kaspersky but (to my knowledge) bypasses a good chunk of other avs.

JoseCmanXDII - March 6, 2022, 9:12 pm

(Mar 6, 2022 02:21 PM)World Wrote: [\[CITE\]](#) If you're melting the exe, I'd recommend using cmd to

copy

Trigger Warning: Ghetto code

```
Code Process.Start("cmd.exe", $"/c copy
```

```
{System.Reflection.Assembly.GetEntryAssembly().Location}' 'c:/droplocation/my.exe");
```

Can't guarantee it would bypass Kaspersky but (to my knowledge) bypasses a good chunk of other avs.

i found that, all this methods are same nothing makes a difference. the problem isnt how i copy the executable to another directory.. the detected part in my case were starting that particular process after copying it or dropping it to other directory so (kaspersky and avast) kills the process and detect it as suspicious. ye i found out that too late i thought its the copying method which did that

(keep in mind that the malware itself is fud so im sure thats the detected part based on other tests aswell)

0x9F - March 6, 2022, 10:51 pm

(Mar 6, 2022 10:12 PM)JoseCmanXDII Wrote: [\[CITE\]](#) i found that, all this methods are same nothing makes a difference. the problem isnt how i copy the executable to another directory.. the detected part in my case were starting that particular process after copying it or dropping it to other directory so (kaspersky and avast) kills the process and detect it as suspicious. ye i found out that too late i thought its the copying method which did that

(keep in mind that the malware itself is fud so im sure thats the detected part based on other tests aswell)

AV vendors usually register kernel callbacks to intercept creation of Processes with PsSetCreateProcessNotifyRoutine, however, it's possible to "outrun" the callback using job objects for process creation. This way you're get your process spawned before triggering the callback.

JoseCmanXDII - March 7, 2022, 2:37 am

(Mar 6, 2022 11:51 PM)0x9F Wrote: [\[CITE\]](#) AV vendors usually register kernel callbacks to intercept creation of Processes with PsSetCreateProcessNotifyRoutine, however, it's possible to "outrun" the callback using job objects for process creation. This way you're get your process spawned before triggering the callback.

thats actually smart ill look into that and tell you thanks