

Forum:[Hack Forums](#)

Thread: [<<<< Easy >>>> How to bypass Windows Defender for beginner in 5min](#)

NYANxCAT - March 14, 2020, 6:33 pm

You all have a problem with WD, I created this video to show you how to bypass WD+Internet easily using open-source runPE class even if you are a beginner!

I also used the browser to download the payload into the WD machine instead of just copy+paste it from VM to another just to simulate the real scenario.

This method will work on .NET or Native files. I did my best to make this tutorial as simple as possible(just 1 class, no external lib, no encryption..etc).

And again.. copy+paste this tutorial won't give you a FUD result, Take the idea and be creative.

Enjoy watching.

Scantime [\(Click to View\)](#)

[Video: <https://www.youtube.com/watch?v=VGwQRkVILb4>]

kausar0707 - March 14, 2020, 7:01 pm

Thanks for sharing dude :)

Aekras1a - March 14, 2020, 7:56 pm

Awesome guide, thank you NYAN, and congratulations on getting married ^^

1stetcgoldmedal - March 14, 2020, 9:04 pm

I respect the spirit of sharing

A great friend for beginners

Mirakuru - March 15, 2020, 4:43 am

Thank you for share mate. :)

Kindness - March 15, 2020, 8:50 am

Very informative and useful tutorial.Thank you so much brother.

Congratulations on getting married.May Allah bless you brother <3

stringsnstuff - March 15, 2020, 12:23 pm

Hello thank you very much Nyan, I have implemented this into my personal runtime/scantime crypter coded in C and it helped for sure. I saw you defined a string for path and a string for decrypting Base64. Do you actually use the Base64 string or do you only have it defined and that's it?

NYANxCAT - March 15, 2020, 12:53 pm

(Mar 15, 2020 12:23 PM)stringsnstuff Wrote: [\[CITE\]](#) Hello thank you very much Nyan, I have implemented this into my personal runtime/scantime crypter coded in C and it helped for sure. I saw you defined a string for path and a string for decrypting Base64. Do you actually use the Base64 string or do you only have it defined and that's it?

hello, yes I used it by converting the string to byte array.

stringsnstuff - March 15, 2020, 1:11 pm

(Mar 15, 2020 12:53 PM)??` NYAN CAT ?`? Wrote: [\[CITE\]](#) hello, yes I used it by converting the string to byte array. Alright sorry for not being clear enough. My question was what did you do with the byte array? I only see the byte array being defined I don't see you using it anywhere.

Irrelewanted - March 16, 2020, 4:23 pm

(Mar 15, 2020 01:11 PM)stringsnstuff Wrote: [\[CITE\]](#) Alright sorry for not being clear enough. My question was what did you do with the byte array? I only see the byte array being defined I don't see you using it anywhere.

Correct me if I'm wrong Nyan, but he executed the "byte array" which was the binary of the RAT (stub) itself.

How he executes the byte array, is a whole and really advanced other story. Look up "process hollowing" on Google for more information on how "RunPE" executes it's code into a newly suspended process.

Great video though. Quick, simple and functioning.

stringsnstuff - March 16, 2020, 4:27 pm

(Mar 16, 2020 04:23 PM)Irrelewanted Wrote: [\[CITE\]](#) Correct me if I'm wrong Nyan, but he executed the "byte array" which was the binary of the RAT (stub) itself.

How he executes the byte array, is a whole and really advanced other story. Look up "process hollowing" on Google for more information on how "RunPE" executes it's code into a newly suspended process.

Great video though. Quick, simple and functioning.

Yeah I know how RunPE works. I know whats going on. He is using the byte array to execute the server. Was confused at first. Thank you for your reply. Was confused because I'm not familiar with this coding language as I am a c++ programmer.

Irrelewanted - March 16, 2020, 4:34 pm

(Mar 16, 2020 04:27 PM)stringsnstuff Wrote: [\[CITE\]](#) Yeah I know how RunPE works. I know whats going on. He is using the byte array to execute the server. Was confused at first. Thank you for your reply.

No problem, I'm glad that I cleared that up for you.

Obistone - March 16, 2020, 6:00 pm

(Mar 16, 2020 04:27 PM)stringsnstuff Wrote: [\[CITE\]](#) Was confused because I'm not familiar with this coding language as I am a c++ programmer.

You should be a little bit familiar with C# as it is in the C family, just like C++.

RedirectMe - March 17, 2020, 8:12 am

C# is not like C++ or C. It's more like Java

kiffu - March 28, 2020, 2:10 am

Thanks for sharing, i tried but WD is detecting, i am not worried about other AVs but i just want to bypass WD, please pm me if you can help and let me know what changes if i do will help me

bypass WD.

Thank You

rainbowlackjack - March 30, 2020, 7:25 pm

i tried this too and windows defender is detecting this method does not work debugged

rkewrefds - March 31, 2020, 3:38 pm

Cant pm but do you have any outside form of contact? I need just a basic rat and crypter that will last me longer than 3 days and I can pay you for pointing me in the right direction, no budget for the rat or crypter. I have bought basically everything on this site and they all dont bypass windows defender longer than like 3-4 days and this is my only requirement. Let me know bro

rainbowlackjack - March 31, 2020, 3:43 pm

will the infected computer still stay connecte if windows defender finds the rat on the installed pc?

martigo333 - April 11, 2020, 7:53 am

(Mar 31, 2020 03:38 PM)rkewrefds Wrote: [\[CITE\]](#) Cant pm but do you have any outside form of contact? I need just a basic rat and crypter that will last me longer than 3 days and I can pay you for pointing me in the right direction, no budget for the rat or crypter. I have bought basically everything on this site and they all dont bypass windows defender longer than like 3-4 days and this is my only requirement. Let me know bro

WD will kill the process and delete it.

djemper89 - April 22, 2020, 2:57 am

Hi. Can you help me ?

[INFO] ConfuserEx v1.0.0 Copyright © Ki 2014

[INFO] Running on Microsoft Windows NT 6.2.9200.0, .NET Framework v4.0.30319.42000, 64 bits

[DEBUG] Discovering plugins...

[INFO] Discovered 10 protections, 1 packers.

[DEBUG] Resolving component dependency...

[INFO] Loading input modules...

[ERROR] Unknown error occurred.

Exception: System.BadImageFormatException: .NET data directory RVA is 0

à dnlib.DotNet.MD.MetadataCreator.Create(IPEImage pelmage, Boolean verify) dans

E:\Source\Public\Confuser2\dnlib\src\DotNet\MD\MetaDataCreator.cs:ligne 176

à dnlib.DotNet.MD.MetadataCreator.Load(String fileName) dans

E:\Source\Public\Confuser2\dnlib\src\DotNet\MD\MetaDataCreator.cs:ligne 32

à Confuser.Core.ObfAttrMarker.MarkProject(ConfuserProject proj, ConfuserContext context) dans

e:\Source\Public\Confuser2\Confuser.Core\ObfAttrMarker.cs:ligne 292

à Confuser.Core.ConfuserEngine.RunInternal(ConfuserParameters parameters,

Cancellation token) dans e:\Source\Public\Confuser2\Confuser.Core\ConfuserEngine.cs:ligne 134

Failed at 11:56, 0:00 elapsed.

seems not to work for C++

Kindness - April 22, 2020, 7:27 am

(Apr 22, 2020 02:57 AM)djemper89 Wrote: [\[CITE\]](#) Hi. Can you help me ?

[INFO] ConfuserEx v1.0.0 Copyright © Ki 2014

[INFO] Running on Microsoft Windows NT 6.2.9200.0, .NET Framework v4.0.30319.42000, 64 bits

[DEBUG] Discovering plugins...

[INFO] Discovered 10 protections, 1 packers.

[DEBUG] Resolving component dependency...

[INFO] Loading input modules...

[_error_] Unknownerror occurred.

Exception: System.BadImageFormatException: .NET data directory RVA is 0

à dnlib.DotNet.MD.MetaDataCreator.Create(IPEImage pelImage, Boolean verify) dans

E:\Source\Public\Confuser2\dnlib\src\DotNet\MD\MetaDataCreator.cs:ligne 176

à dnlib.DotNet.MD.MetaDataCreator.Load(String fileName) dans

E:\Source\Public\Confuser2\dnlib\src\DotNet\MD\MetaDataCreator.cs:ligne 32

à Confuser.Core.ObfAttrMarker.MarkProject(ConfuserProject proj, ConfuserContext context) dans

e:\Source\Public\Confuser2\Confuser.Core\ObfAttrMarker.cs:ligne 292

à Confuser.Core.ConfuserEngine.RunInternal(ConfuserParameters parameters,

CancellationToken token) dans e:\Source\Public\Confuser2\Confuser.Core\ConfuserEngine.cs:ligne 134

Failed at 11:56, 0:00 elapsed.

seems not to work for C++

See this screenshot it may help you to understand why it doesn't work with C++.It works only

.NET applications.

<https://prnt.sc/s414wh>

Thanks

KenUchicha7 - April 24, 2020, 1:50 am

3:10 when youre a hyperactive programmer lol

heymarti - July 7, 2020, 8:36 am

Thanks for passing on your knowledge, I'll try to do it too ... XD

lululululu - July 8, 2020, 1:12 pm

With your help, i wrote my own runpe and my own crypter, thanks for sharing your experience

(Mar 31, 2020 03:38 PM)rkewrefds Wrote: [\[CITE\]](#) Cant pm but do you have any outside form of contact? I need just a basic rat and crypter that will last me longer than 3 days and I can pay you for pointing me in the right direction, no budget for the rat or crypter. I have bought basically everything on this site and they all dont bypass windows defender longer than like 3-4 days and this is my only requirement. Let me know bro

I would recommand to let your loader download the payload from a server:

1. Antivirus will take longer to detect your stuff, if you do it right
2. You can easily update your payload

papyrus2025 - November 6, 2020, 9:23 am

Thanks for sharing dude :)

socialie - November 9, 2020, 6:05 am

The youtube link is out :(

SIM-4686057 - November 28, 2020, 9:25 am

Thanks for sharing mate thanks