

## Forum:[Hack Forums](#)

Thread: [Simple .NET Malware Loader](#)

**NYANxCAT** - August 13, 2018, 12:54 pm

Hello,

I noticed that VB.NET section is inactive recently, And also didn't see any loader so I want to share with you guys a very simple and straightforward .NET loader. Just to post something here. But I would love to see some suggestions, TBH I'm not that good lol.

[:: Download Link ::](#)

**RCE** - August 13, 2018, 1:03 pm

Thanks for sharing this, however, dropping files and spawning process from resources will trigger most of the time

AV's proactive defense also i liked the ur method to set values in register with a non-traditional method by using StrReverse function.

Good Job .

**NYANxCAT** - August 13, 2018, 1:29 pm

(Aug 13, 2018 01:03 PM)ShadoBIH Wrote: [\[CITE\]](#) Thanks for sharing this, however, dropping files and spawning process from resources will trigger most of the time

AV's proactive defense also i liked the ur method to set values in register with a non-traditional method by using StrReverse function.

Good Job .

Thanks for your feedback, I really appreciate it. ?

There are many methods for dropping files but this is the simplest one, however, I always use the startup folder as a drop method for my everyday testing just to make sure that I'm making the loader to be super aggressive, and have no issue with the runtime scan always bypass, But I what noticed is that AV trigger sometimes for this 2 lines

```
Code Diagnostics.Process.Start(Path_)
```

```
Environment.Exit(0)
```

Again, Thanks for feedback ?

**Crytic Coder..** - August 13, 2018, 2:08 pm

(Aug 13, 2018 12:54 PM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) Hello,

I noticed that VB.NET section is inactive recently, And also didn't see any loader so I want to share with you guys a very simple and straightforward .NET loader. Just to post something here. But I would love to see some suggestions, TBH I'm not that good lol.

[:: Download Link ::](#)

(Aug 13, 2018 01:03 PM)ShadoBIH Wrote: [\[CITE\]](#) Thanks for sharing this, however, dropping files and spawning process from resources will trigger most of the time  
AV's proactive defense also i liked the ur method to set values in register with a non-traditional method by using StrReverse function.

Good Job .

(Aug 13, 2018 01:29 PM)??` NYAN CAT ?`? Wrote: [\[CITE\]](#) Thanks for your feedback, I really appreciate it. ?

There are many methods for dropping files but this is the simplest one, however, I always use the startup folder as a drop method for my everyday testing just to make sure that I'm making the loader to be super aggressive, and have no issue with the runtime scan always bypass, But I what noticed is that AV trigger sometimes for this 2 lines

```
Code Diagnostics.Process.Start(Path_  
Environment.Exit(0)
```

Again, Thanks for feedback ?

Enough with the .NET malware, I can make one in 10 Minutes with like 5 features and make a crypter to wrap it.. I'd be the richest due of hf..I bet my life on it..

**NYANxCAT** - August 13, 2018, 2:18 pm

(Aug 13, 2018 02:08 PM)Crytic Coder.. Wrote: [\[CITE\]](#) Enough with the .NET malware, I can make one in 10 Minutes with like 5 features and make a crypter to wrap it.. I'd be the richest due of hf..I bet my life on it..

Hello,

I suppose you didn't read my first and only paragraph, I shall quote it so you read it, sir.

Quote:I noticed that VB.NET section is inactive recently, And also didn't see any loader so I want to share with you guys a very simple and straightforward .NET loader. Just to post something here.

Quote:Enough with the .NET

As you see, This is the .NET section, You will only find .NET threads. lol, It's like I'm teaching you A B C D this should be obvious It's .NET section

EDIT:

PHP Code

```
<?php
```

Reputation: -19

geez...

**Crytic Coder..** - August 13, 2018, 2:31 pm

(Aug 13, 2018 02:18 PM)??` NYAN CAT ?`? Wrote: [\[CITE\]](#) Hello,

I suppose you didn't read my first and only paragraph, I shall quote it so you read it, sir.

As you see, This is the .NET section, You will only find .NET threads. lol, It's like I'm teaching you A B C D this should be obvious It's .NET section

EDIT:  
PHP Code  
<?php  
Reputation: -19  
geez...  
Hit dat E G H babe

**NYANxCAT** - August 13, 2018, 2:33 pm

(Aug 13, 2018 02:31 PM)Crytic Coder.. Wrote: [\[CITE\]](#) Hit dat E G H babe

PHP Code  
<?php  
Reputation: -22  
GEEZ.. it was 19 like 5 min ago... ???

**Washi** - August 14, 2018, 4:07 am

While I know nothing about removing detections because I am really not interested in that topic, I got a couple of comments on your source code:

You're probably one of the first people here that uses Path.Combine in their source code. Good job!

What's up with all the shared variables? Always try to minimise the scope each variable is accessible to. E.g. Count is only used in the Sleeping function. It would therefore make sense to declare it inside Sleeping rather than in global scope.

What is the point of the Sleeping function in the first place? It always returns true, meaning your if statement in Main is pretty pointless, and it always sleeps for 5 seconds? Couldn't you just have used Thread.Sleep(1000 \* 5) in your Main method?

I see every member in a class is marked as Shared. Consider using Module instead of Class which marks all members Shared without explicitly specifying so.

I assume the 35 in Environment.GetFolderPath(35) is used instead of the direct enum field as a means of obfuscation? While it might be effective upon reading the source code, it doesn't matter at low level. Pretty much every decompiler will detect the 35 as a constant that is related to the SpecialFolder.CommonApplicationData enum field, and replace it with the enum constant instead. A rule of thumb is to prefer readability of source code over shortcuts and brevity, which you might want to consider following as well.

In your encryption and compression functions, you are using quite a few instances that implement the [IDisposable](#) interface. While you do dispose them, this is not guaranteed to be invoked once an exception occurs. Therefore, always wrap your disposable variables in a Using statement unless you have a really good reason not to.

Also there doesn't seem to be any instructions in the thread on how to use it? There are a few comments here and there in the source code, but it does not really give any explanation on what to change to make it work.

Just my thoughts.

(Aug 14, 2018 04:07 AM)Washi Wrote: [\[CITE\]](#) While I know nothing about removing detections because I am really not interested in that topic, I got a couple of comments on your source code: You're probably one of the first people here that uses Path.Combine in their source code. Good job!

What's up with all the shared variables? Always try to minimise the scope each variable is accessible to. E.g. Count is only used in the Sleeping function. It would therefore make sense to declare it inside Sleeping rather than in global scope.

What is the point of the Sleeping function in the first place? It always returns true, meaning your if statement in Main is pretty pointless, and it always sleeps for 5 seconds? Couldn't you just have used Thread.Sleep(1000 5) in your Main method?

I see every member in a class is marked as Shared. Consider using Module instead of Class which marks all members Shared without explicitly specifying so.

I assume the 35 in Environment.GetFolderPath(35) is used instead of the direct enum field as a means of obfuscation? While it might be effective upon reading the source code, it doesn't matter at low level. Pretty much every decompiler will detect the 35 as a constant that is related to the SpecialFolder.CommonApplicationData enum field, and replace it with the enum constant instead. A rule of thumb is to prefer readability of source code over shortcuts and brevity, which you might want to consider following as well.

In your encryption and compression functions, you are using quite a few instances that implement the [IDisposable](#) interface. While you do dispose them, this is not guaranteed to be invoked once an exception occurs. Therefore, always wrap your disposable variables in a Using statement unless you have a really good reason not to.

Also there doesn't seem to be any instructions in the thread on how to use it? There are a few comments here and there in the source code, but it does not really give any explanation on what to change to make it work.

Just my thoughts.

This is really HQ post, rep+ for this, I really appreciate any help or suggestion since I'm new to loaders.

Quote:[\*]What's up with all the shared variables? Always try to minimise the scope each variable is accessible to. E.g. Count is only used in the Sleeping function. It would therefore make sense to declare it inside Sleeping rather than in global scope.

Here I agree with you, I should use declare dim count inside sleeping function, I think it's just a habit ???

Quote:[\*]What is the point of the Sleeping function in the first place? It always returns true, meaning your if statement in Main is pretty pointless, and it always sleeps for 5 seconds? Couldn't you just have used Thread.Sleep(1000 5) in your Main method?

I will quote a post from another thread of mine.

<http://prntscr.com/kimc06>

So instead of the whole application is sleeping, I'm doing a loop so the function is working and not sleeping but in same time it sleeps for 1sec every loop. I don't know if this really work to add evasion or not.

Quote:[\*]I see every member in a class is marked as Shared. Consider using Module instead of Class which marks all members Shared without explicitly specifying so.

Yeah, modules are great in VB. But don't usually use

Quote:[\*]I assume the 35 in Environment.GetFolderPath(35) is used instead of the direct enum field as a means of obfuscation? While it might be effective upon reading the source code, it doesn't matter at low level. Pretty much every decompiler will detect the 35 as a constant that is related to the SpecialFolder.CommonApplicationData enum field, and replace it with the enum constant instead. A rule of thumb is to prefer readability of source code over shortcuts and brevity, which you might want to consider following as well.

To be honest, it wasn't about obfuscation, I'm trying to learn to use numbers instead of the special folder to make my line shorter and cleaner.

Quote:Also there doesn't seem to be any instructions in the thread on how to use it? There are a few comments here and there in the source code, but it does not really give any explanation on what to change to make it work.

Another bad habit, I don't put comments on my projects even in github, But I tried to make everything read-able for example

Cryptography\_  
AESDecrypt\_(File As Byte, Pass As String)

**Pikachu** - August 14, 2018, 3:04 pm

This is a pretty good contribution OP! Nice work!

**NYANxCAT** - August 14, 2018, 3:11 pm

(Aug 14, 2018 03:04 PM)Mimikyu Wrote: [\[CITE\]](#) This is a pretty good contribution OP! Nice work! Thanks, I appreciate your support ?

**Washi** - August 14, 2018, 3:28 pm

(Aug 14, 2018 12:26 PM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) I will qoute a post from another thread of mine.

<http://prntscr.com/kimc06>

So instead of the whole application is sleeping, I'm doing a loop so the function is working and not sleeping but in same time it sleeps for 1sec every loop. I don't know if this really work to add evasion or not.

Could be. Again, I have no idea about this.

(Aug 14, 2018 12:26 PM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) Yeah, modules are great in VB. But don't usually use.

Why not?

(Aug 14, 2018 12:26 PM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) To be honest, it wasn't about obfuscation, I'm trying to learn to use numbers instead of the special folder to make my line shorter

and cleaner.

You should definitely not get used to that! Using the enum constants over raw magic numbers greatly improve readability of your source code. Always imagine yourself reading this source code a few months / years later. You should still be able to understand it from the get go. Magic constants don't help with that :)

**NYANxCAT** - August 14, 2018, 3:39 pm

(Aug 14, 2018 03:28 PM)Washi Wrote: [\[CITE\]](#) Could be. Again, I have no idea about this.Yeah me too, evading AV is a subject, and writing a normal application is another subject

(Aug 14, 2018 03:28 PM)Washi Wrote: [\[CITE\]](#) Why not?I only use Modules When I need to use some methods continuously on heavy projects, But for this loader, I thought there is no need for it.

(Aug 14, 2018 03:28 PM)Washi Wrote: [\[CITE\]](#) You should definitely not get used to that! Using the enum constants over raw magic numbers greatly improve readability of your source code. Always imagine yourself reading this source code a few months / years later. You should still be able to understand it from the get go. Magic constants don't help with that :)? hmmm, I didn't think about this, I guess you are right

**Ph3n0mz** - August 15, 2018, 12:32 pm

I tested this by trying to load my RAT server but it's not working, is there anything i'm doing wrong? Is there something i don't know about? Should it be working with a RAT? Thanks to anyone who's going to help me understand.

**NYANxCAT** - August 15, 2018, 2:56 pm

(Aug 15, 2018 12:32 PM)Ph3n0mz Wrote: [\[CITE\]](#) I tested this by trying to load my RAT server but it's not working, is there anything i'm doing wrong? Is there something i don't know about? Should it be working with a RAT? Thanks to anyone who's going to help me understand.

Hello,

Did you use the gzip+aes on your payload? I left them at the bottom of my loader. Yes it should work.

**Ph3n0mz** - August 16, 2018, 9:05 am

(Aug 15, 2018 02:56 PM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) Hello,

Did you use the gzip+aes on your payload? I left them at the bottom of my loader. Yes it should work.

Hi, thanks for replying, could you help me a little with this? I did replace "IMG2" with my server (since it's the payload), added it to the resources, compiled and it didn't run my server..

**NYANxCAT** - August 16, 2018, 11:41 am

(Aug 16, 2018 09:05 AM)Ph3n0mz Wrote: [\[CITE\]](#) Hi, thanks for replying, could you help me a little with this? I did replace "IMG2" with my server (since it's the payload), added it to the resources, compiled and it didn't run my server..

Hello,

Sir did you read the whole source? You need to manually use ass encryption and gzip.

It's very easy thing to do.

IMG2 must be encrypted.

?

**Ph3n0mz** - August 16, 2018, 1:06 pm

(Aug 16, 2018 11:41 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) Hello,

Sir did you read the whole source? You need to manually use ass encryption and gzip.

It's very easy thing to do.

IMG2 must be encrypted.

?

Oh my god... Alright thanks for the info! I was just trying to test it without any encryption at all i guess it was the problem ^.^

**NYANxCAT** - August 16, 2018, 2:12 pm

(Aug 16, 2018 01:06 PM)Ph3n0mz Wrote: [\[CITE\]](#) Oh my god... Alright thanks for the info! I was just trying to test it without any encryption at all i guess it was the problem ^.^

Yes you need to use these two function, or you could just delete them and use base64

**InterGalactic** - August 17, 2018, 10:34 am

I already download it, NiC3!

**NYANxCAT** - August 17, 2018, 12:06 pm

(Aug 17, 2018 10:34 AM)InterGalactic Wrote: [\[CITE\]](#) I already download it, NiC3!

Glad you like it ?

**Kufe** - August 19, 2018, 1:25 am

Nyan cat, can you please PM me, I have a few questions I would like to ask you but can't send you PM myself.

**emmabee** - August 19, 2018, 7:23 am

Many thanks NyanCat....always interesting to learn anothe way of doing things

**Xogg** - August 19, 2018, 3:51 pm

oops it no longer works!

Just a joke dont hurt me,

on a real note. Other than framework dependent code; Nice work!

**NYANxCAT** - August 19, 2018, 8:30 pm

(Aug 19, 2018 03:51 PM)ParadoxTheDev Wrote: [\[CITE\]](#)

oops it no longer works!

Just a joke dont hurt me,

on a real note. Other than framework dependent code; Nice work!

lool thanks man ?

(Aug 19, 2018 01:25 AM)Kufe Wrote: [\[CITE\]](#) Nyan cat, can you please PM me, I have a few questions I would like to ask you but can't send you PM myself.Pmed

(Aug 19, 2018 07:23 AM)emmabee Wrote: [\[CITE\]](#) Many thanks NyanCat....always interesting to learn anothe way of doing thingsI hope I could help.

**OffCode** - August 20, 2018, 9:35 am

Wouu, Very nice work!

Keep up good work!

**Pesto50** - August 21, 2018, 8:55 am

Very good contribution! I think .NET is dying due to the popularity of other languages (NodeJS, Python)

**m4ll0c** - February 12, 2019, 4:27 am

I like Your cat, jumping over the sky and stars! LOL

**Bitcoiner** - October 29, 2019, 2:16 am

thanks for sharing, good....

**MavenGradle** - October 29, 2019, 11:58 am

(Oct 29, 2019 09:51 AM)Wikipedia Wrote: [\[CITE\]](#) Microsoft rolled out .NET Core awhile ago to move the .NET Framework to other operating systems like Linux, so the use of the .NET Framework will continue to increase as opposed to decrease.

This statement is entirely incorrect and indicates to me that you may not have researched the things you're talking about. Let me explain why.

.NET Core & .NET Framework are very different products. The usage of .NET Framework will not continue to increase as .NET Core is intended to replace the .NET Framework entirely. So, long term, you'll see a decline in .NET Framework applications.

Here's a graph that should explain it all, including .NET Standard:

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

Noted, this graph is out-of-date and should now include WPF and WinForms in .NET Core as well. Granted, both WPF and WinForms in .NET Core will only work on Windows at the moment.

If you want to take this all one step further, let's look into future releases of both .NET Core and .NET Framework. We'll see there's now a thing in the making called .NET 5 which will be the only platform going forward:

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

So, unless Microsoft changes their plans, you will see only .NET applications in the future. .NET 5 will be built using 'the best' of .NET Core 3, Framework, Xamarin and Mono so the .NET Framework in the traditional sense will be entirely obsolete:

<https://devblogs.microsoft.com/dotnet/introducing-net-5/>

**MavenGradle** - October 29, 2019, 1:50 pm

(Oct 29, 2019 12:11 PM)Wikipedia Wrote: [\[CITE\]](#) I assumed that the .NET Core would have been re-using things from the .NET Framework.

That assumption would have been correct. Microsoft is re-using certain implementations of features and functions. They claim so themselves, except they are improving upon said functions and features, whatever they understand under the word 'improving'.