

Forum:[Hack Forums](#)

Thread: [Xworm plugin error](#)

Rs6 - February 10, 2026, 11:33 pm

Hello to all ?

Can anyone recommend a crypter that is xworm 6.0 compatible and has no problem with plugins?
I mean no errors of this type when you try to open a plugin on the client:

Plugin error!Could not load file or assembly '1633280 bytes loaded from XWormClient,Version=1.0.0.0,Culture=neutral,PublicKeyToken=null' or one of its dependencies. An attempt was made to load a program with an incorrect format.

Thanks in advance.

R5N3T - February 10, 2026, 11:45 pm

Hopefully someone here can help you out with this, bro.

ServersFxcked - February 11, 2026, 3:07 am

Wouldn't use anything passed 5.6 as its not the real xCoder

CL1B - February 11, 2026, 3:09 am

(Feb 11, 2026 04:07 AM)ServersFxcked Wrote: [\[CITE\]](#) Wouldn't use anything passed 5.6 as its not the real xCoder

^

jmark7 - February 11, 2026, 11:34 am

thats is runtime detection from windows defender when the plugin is loaded.

No Crypter can bypass it, Only way to bypass is to re-fud the plugins.

You can PM me with your TG ID if you need professional solution on it.

Pankii - February 11, 2026, 2:07 pm

You have been caught by Amsi. You have to obfuscate your xworm DLL's or add amsi bypass in your client code. The second option might be worse than first but it makes permanent solution.

gvnscrutinizer - February 11, 2026, 2:39 pm

AMSI are scanning the plugin bytes.

(Feb 11, 2026 12:34 PM)jmark7 Wrote: [\[CITE\]](#) thats is runtime detection from windows defender when the plugin is loaded.

No Crypter can bypass it, Only way to bypass is to re-fud the plugins.

You can PM me with your TG ID if you need professional solution on it.

Not true- you just need an amsi bypass that propagates for all sequential plugin loads by the rat payload

(Feb 11, 2026 12:45 AM)R5N3T Wrote: [\[CITE\]](#) Hopefully someone here can help you out with this, bro.

its due to using a mid tier crypter which doesnt consider runtime activity from the payload itself i.e.

loading plugins. the payload itself may have not triggered amsi but xworm loads plugins via `assembly.load(byte)` which get scanned by amsi.

CL1B - February 12, 2026, 4:04 am

What's up with everyone thinking this has anything to do with AMSI?

The bytes have been loaded already, you guys clearly do not know how AMSI works.

This is caused by arch mismatching and nothing else, if you have the source code; Compile the stub and plugins in the same x64 arch.

In some cases (especially when dealing with old projects) there will a missing dependency, you can easily find, download and add this using dependency walker or fus log viewer.

For those who don't know how AMSI works; Go to mimikatz PS github and use the script command, watch how loud AMSI screams it's name.

Much different.

Frost Crypt - February 12, 2026, 4:17 am

(Feb 12, 2026 05:04 AM)MarlboroMan Wrote: [\[CITE\]](#) What's up with everyone thinking this has anything to do with AMSI?

The bytes have been loaded already, you guys clearly do not know how AMSI works.

This is caused by arch mismatching and nothing else, if you have the source code; Compile the stub and plugins in the same x64 arch.

In some cases (especially when dealing with old projects) there will a missing dependency, you can easily find, download and add this using dependency walker or fus log viewer.

For those who don't know how AMSI works; Go to mimikatz PS github and use the script command, watch how loud AMSI screams it's name.

Much different.

because it does most likely, I'm getting a very similar detection when my .net file is loaded into memory in powershell via `[System.Reflection.Assembly]::Load($...)`;
When that happens I have to refud it to fix it.

Exception calling "Load" with "1" argument(s): "Could not load file or assembly '50688 bytes loaded from Anonymously Hosted DynamicMethods Assembly, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null' or one of its dependencies. An attempt was made to load a program with an incorrect format."

This is what I'm getting and WD blocks it SILENTLY, you need to keep wd opened to see the detection, there is no notification.

So if xworm is storing these plugins as bytes, wd tagged them and gives that silent detection when you're trying to load them.

So try to lose some of your big balls attitude because you don't know half as much as you think you know and bullying others while being wrong is pretty embarrassing.

Op can use any crypter he wants, until those plugins are refuted, they will fail to load.

CL1B - February 12, 2026, 4:45 am

OP, You're better off with a stack overflow search.

Trust.

gvnscrutinizer - February 12, 2026, 7:25 am

(Feb 12, 2026 05:04 AM)MarlboroMan Wrote: [\[CITE\]](#) What's up with everyone thinking this has anything to do with AMSI?

The bytes have been loaded already, you guys clearly do not know how AMSI works.

This is caused by arch mismatching and nothing else, if you have the source code; Compile the stub and plugins in the same x64 arch.

In some cases (especially when dealing with old projects) there will a missing dependency, you can easily find, download and add this using dependency walker or fus log viewer.

For those who don't know how AMSI works; Go to mimikatz PS github and use the script command, watch how loud AMSI screams it's name.

Much different.

You're so confidently wrong lmao. xworm and many other modular rats load plugins reflectively via `assembly.load(byte[])`. xworm is heavily signed so the bytes get scanned by AMSI and blocked

possessed-client - February 12, 2026, 7:56 am

(Feb 11, 2026 12:33 AM)Rs6 Wrote: [\[CITE\]](#) Hello to all ?

Can anyone recommend a crypter that is xworm 6.0 compatible and has no problem with plugins? I mean no errors of this type when you try to open a plugin on the client:

Plugin error!Could not load file or assembly '1633280 bytes loaded from XWormClient,Version=1.0.0.0,Culture=neutral,PublicKeyToken=null' or one of its dependencies. An attempt was made to load a program with an incorrect format.

Thanks in advance.

Well, flame wars notwithstanding, it's easy to figure out whether the problem is with AV detecting plugins or something else by testing in a VM with and without AV protection. And if it is AV, then yeah, you either have to FUD the plugins by modifying source and recompiling or trying various obfuscators. Alternatively, you have to bypass AMSI for the process trying to load the plugin, and if the plugin is detected even on disk before execution, then you have to rewrite how the RAT handles plugins, so it bypasses AMSI, then decrypts the plugin and only then loads and runs it.

Here's a recent topic with a similar problem: <https://hackforums.net/showthread.php?tid=6317704>

Your idea of using a crypter might work if it has a working AMSI bypass and the plugin isn't detected on disk (or maybe even in memory) before AMSI gets into play with `Assembly.Load` call to the plugin path or variable in memory.

Rs6 - February 13, 2026, 8:10 am

Thanks to all for answers.

So if i understand correctly, i need to find or crypter that bypasses AMSI or way to obfuscate

plugins?

gvnscrutinizer - February 13, 2026, 10:33 am

(Feb 13, 2026 09:10 AM)Rs6 Wrote: [\[CITE\]](#) Thanks to all for answers.

So if i understand correctly, i need to find or crypter that bypasses amsi or way to obfuscate plugins?

yup. send me a pm if you want help with confirming its amsi blocking plugin loads and what would needa be done.

Frost Crypt - February 13, 2026, 10:12 pm

(Feb 13, 2026 09:10 AM)Rs6 Wrote: [\[CITE\]](#) Thanks to all for answers.

So if i understand correctly, i need to find or crypter that bypasses amsi or way to obfuscate plugins?

you need to crypt better maintained products or find someone to refud those plugins otherwise you will just waste money on crypters

akusayan - February 15, 2026, 8:26 am

m using xworm from years i face this error when my payload is detected
use Process exclusion in defender

Rs6 - February 15, 2026, 10:49 pm

(Feb 15, 2026 09:26 AM)akusayan Wrote: [\[CITE\]](#) m using xworm from years i face this error when my payload is detected

use Process exclusion in defender

This is a clever solution, but how do i do it when the plugins dont work?

possessed-client - February 16, 2026, 4:17 am

(Feb 15, 2026 11:49 PM)Rs6 Wrote: [\[CITE\]](#) This is a clever solution, but how do i do it when the plugins dont work?

You'll need a crypter that can do exclusions (that can deal with tamper protection, otherwise very low success percentage nowadays - only on multiple years old Win 10) or bind your payload in whatever way with a module that deals with exclusion - I know of two methods, one is using defendnot from Github and then adding the exclusion, other is using BYOVD to kill WD processes then adding the exclusion.

Rs6 - February 16, 2026, 5:25 am

(Feb 16, 2026 05:17 AM)possessed-client Wrote: [\[CITE\]](#) You'll need a crypter that can do exclusions (that can deal with tamper protection, otherwise very low success percentage nowadays - only on multiple years old Win 10) or bind your payload in whatever way with a module that deals with exclusion - I know of two methods, one is using defendnot from Github and then adding the exclusion, other is using BYOVD to kill WD processes then adding the exclusion.

Crypter with exclusion on hole /C ,or with some other parameters?

possessed-client - February 16, 2026, 5:27 am

(Feb 16, 2026 06:25 AM)Rs6 Wrote: [\[CITE\]](#) Crypter with exclusion on hole /C ,or with some other parameters?

I mean, excluding the whole drive should work, but it also increases the chance of you getting more 'neighbours' on the system, so ideally you'd only exclude specific directories relevant to your payload.

Rs6 - February 16, 2026, 5:44 am

(Feb 16, 2026 06:27 AM)possessed-client Wrote: [\[CITE\]](#) I mean, excluding the whole drive should work, but it also increases the chance of you getting more 'neighbours' on the system, so ideally

you'd only exclude specific directories relevant to your payload.

Thanks for advice buddy ??

Rs6 - February 19, 2026, 8:40 am

Can anyone recommend a crypter with amsi bypass or wd exclusion and outputted extension .js ?

Frost Crypt - February 19, 2026, 8:51 am

(Feb 19, 2026 09:40 AM)Rs6 Wrote: [\[CITE\]](#) Can anyone recommend a crypter with amsi bypass or wd exclusion and outputted extension .js ?

exclusion is added based on some path on your drive, this is MEMORY detection so is located just in ram so adding like C drive to exclusion will still trigger WD, it might work if you exclude the detection name directly if you can, just so you know