

Forum:[Hack Forums](#)

Thread: [\[EXCLUSIVE\] Forever Fud .NET](#)

skyt__ - September 19, 2025, 7:48 pm

Hello HF,

Just wanted to give a little update on my .NET crypter journey. I was originally going to do some UI application for the crypter but I figured a telegram bot would be more efficient. In a week or two I will have pooled together enough resources to make the release of Forever Fud official. It will be private and only 10 license keys will be available. It will be 0/72 detections on virustotal forever as long as the executable generated is not uploaded to virus total too many times. Stay tuned!

webdev77 - September 19, 2025, 8:28 pm

In today's modern world with AV tools relying upon cloud-based data sharing and sampling, I think virustotal is the least of your concerns. In any case, happy developing on your journey.

DramaKing - September 20, 2025, 5:16 am

Or downloaded too many times.

skyt__ - September 20, 2025, 7:06 am

(Sep 20, 2025 05:16 AM)DramaKing Wrote: [\[CITE\]](#) Or downloaded too many times.

Can you elaborate? Because when the executable is statically analyzed it will never be detected. But of course if its ran through a sandbox it will display the malicious behavior.

ServersFucked - September 21, 2025, 12:18 am

But you say that like the people that get sent it wont upload it

skyt__ - September 21, 2025, 6:43 am

(Sep 21, 2025 12:18 AM)ServersFucked Wrote: [\[CITE\]](#) But you say that like the people that get sent it wont upload it

Honestly, if people are that adamant about uploading it I dont fucking care just upload it I guess ?

MadScientist - September 22, 2025, 10:14 am

(Sep 21, 2025 06:43 AM)skyt__ Wrote: [\[CITE\]](#) Honestly, if people are that adamant about uploading it I dont fucking care just upload it I guess ?

Even end users may upload it, I upload anything I download off the web (aside from things I know and trust/some tools) to VT before I run it.

skyt__ - September 23, 2025, 3:23 pm

(Sep 22, 2025 10:14 AM)MadScientist Wrote: [\[CITE\]](#) Even end users may upload it, I upload anything I download off the web (aside from things I know and trust/some tools) to VT before I run it. Sure ?

Hackers - September 25, 2025, 10:39 am

(Sep 19, 2025 08:28 PM)webdev77 Wrote: [\[CITE\]](#) In today's modern world with AV tools relying upon cloud-based data sharing and sampling, I think virustotal is the least of your concerns. In any case, happy developing on your journey.

This is the thing people aren't understanding fully...

It does not matter what you do in userland, frontend, install process, runtime, etc...

You can detect patterns in kernel, minifilter, etc and flag susp activity.

If it doesn't have a cert, it's getting scanned regardless.

If it does have a cert and that cert is new, it's getting scanned

AAAAAAAND if it has a "trusted" cert, it's still getting scanned for a good bit anyways.
and if that trusted, certified program has any ability to run other programs/files, or sideloading access.... it's getting scanned every time.

This isn't always 100% true for every single AV, but it's pretty true.

They don't need sigs, static analysis, etc

If someone's shooting you, do you look to see if they're holding a gun, or do you look down at the bullet hole in your stomach?

Kernel monitoring is the bullet hole, they don't care how you get your prog started / in runtime.

Of course, methods always exist... But the idea of "forever FUD" is silly.... In .NET too

And lastly, even if you do achieve FUD reliably, you still need to get through MOTW, SmartScreen, etc.

So lets say you do that... It only takes 1 user with good security to flag & auto-upload your prog for analysis.

If you can build a FUD crypter, you can do a lot more.

Look into whitehat embedded systems, encryption work, protected runtimes, and more - hell, you could even think about going into cybersecurity / defense.

That's ultimately my advice to any crypter dev. If you can crypt, you can do a lot more with your life. Don't limit yourself

skyt__ - September 25, 2025, 1:37 pm

(Sep 25, 2025 10:39 AM)nodes Wrote: [\[CITE\]](#) This is the thing people aren't understanding fully...

It does not matter what you do in userland, frontend, install process, runtime, etc...

You can detect patterns in kernel, minifilter, etc and flag susp activity.

If it doesn't have a cert, it's getting scanned regardless.

If it does have a cert and that cert is new, it's getting scanned

AAAAAAAND if it has a "trusted" cert, it's still getting scanned for a good bit anyways.
and if that trusted, certified program has any ability to run other programs/files, or sideloading access.... it's getting scanned every time.

This isn't always 100% true for every single AV, but it's pretty true.

They don't need sigs, static analysis, etc

If someone's shooting you, do you look to see if they're holding a gun, or do you look down at the bullet hole in your stomach?

Kernel monitoring is the bullet hole, they don't care how you get your prog started / in runtime.

Of course, methods always exist... But the idea of "forever FUD" is silly.... In .NET too

And lastly, even if you do achieve FUD reliably, you still need to get through MOTW, SmartScreen, etc.

So lets say you do that... It only takes 1 user with good security to flag & auto-upload your prog for analysis.

If you can build a FUD crypter, you can do a lot more.

Look into whitehat embedded systems, encryption work, protected runtimes, and more - hell, you could even think about going into cybersecurity / defense.

That's ultimately my advice to any crypter dev. If you can crypt, you can do a lot more with your life. Don't limit yourself

Thank you very much for all the info! Fyi it does bypass smart screen, windows defender, etc and isnt detected by any antivirus so far. Quite frankly, I wouldnt even call it a crypter. It's purely like some sort of a bypass. Extremely little coding necessary took me around ?200-300 lines. So please don't give me too much credit as my friend gave me the initial like part of the "method" but I transformed it into being accessible for .NET assemblies?. "Forever Fud" is just a name btw I thought it was catchy. I appreciate your support.

Hackers - September 25, 2025, 2:38 pm

(Sep 25, 2025 01:37 PM)skyt__ Wrote: [CITE](#) Thank you very much for all the info! Fyi it does bypass smart screen, windows defender, etc and isnt detected by any antivirus so far. Quite frankly, I wouldnt even call it a crypter. It's purely like some sort of a bypass. Extremely little coding necessary took me around ?200-300 lines. So please don't give me too much credit as my friend gave me the initial like part of the "method" but I transformed it into being accessible for .NET assemblies?. "Forever Fud" is just a name btw I thought it was catchy. I appreciate your support. Probably flagged, but Microsoft specifically said that this chain method is NOT a vulnerability:

<https://hackforums.net/showthread.php?tid=6291588>

They say that the UAC methods used in that method are NOT a vuln because they only work if the user could approve admin perms (they say this for most UAC methods).

It was tricky to figure out but it did work well when I made that thread.

You might find it useful

If you're looking for other fun projects.... I linked to a bunch of my past prototypes here:

<https://hackforums.net/showthread.php?tid=6308600&pid=62824237#pid62824237>