

Forum:[Hack Forums](#)

Thread: [How FUD\(Fully UnDetectable\) A C# Program](#)

tra_extra - July 6, 2017, 9:32 am

Hi there,

I wrote a good program for spying.

It creates three assemblies & installs them on three different places on windows.

My problem is [VirusTotal](#) & [Windows Defender](#) on Windows 10.

They recognize my program as virus.

Now here i am to starting for FUD job & i don't know where should i study & how can i start?

Please show me the ways & help me to FUD my codes & keep them FUD always.

I heard about SandBox method!

Does it really work & how can i apply it on my project with c# language?

+++++

So in this thread show us :

1- All ways for FUD a C# project.

2- Attach any Codes if exist related to your method.

3- Tell us about SandBox & show us some projects related to it.

maldev0 - July 6, 2017, 9:35 am

Comment partial code blocks out and keep scanning until you find the code block which causes the detection(s). Find a workaround then.

tra_extra - July 6, 2017, 9:39 am

After finding that block(s) what should i do?

I can't remove it(them) & keep comment(s) because i will lost functionality of my codes.

St?Ik?r - July 6, 2017, 9:43 am

(Jul 6, 2017 09:39 AM)tra_extra Wrote: [\[CITE\]](#) After finding that block(s) what should i do?

I can't remove it(them)!!!

You have to recode this partor find a other way. The second thing is NEVER scan malware on virustotal use sites like <https://nodistribute.com/> or <http://xcscan.com/> (1 Free scan a day / 100 credits = 1\$ / Scan = 3 credits = 33 scans for 1\$)

tra_extra - July 6, 2017, 9:48 am

(Jul 6, 2017 09:43 AM)St?Ik?r Wrote: [\[CITE\]](#) You have to recode this partor find a other way. The second thing is NEVER scan malware on virustotal use sites like <https://nodistribute.com/> or <http://xcscan.com/> (1 Free scan a day / 100 credits = 1\$ / Scan = 3 credits = 33 scans for 1\$) 33 scans for 1\$ > Is this real > Or just a SEO trick?

M?xim - July 6, 2017, 9:50 am

(Jul 6, 2017 09:43 AM)St?Ik?r Wrote: [\[CITE\]](#) You have to recode this partor find a other way. The second thing is NEVER scan malware on virustotal use sites like <https://nodistribute.com/> or <http://xcscan.com/> (1 Free scan a day / 100 credits = 1\$ / Scan = 3 credits = 33 scans for 1\$) Here's a good thread for that topic: <https://hackforums.net/showthread.php?tid=5639786>

maldev0 - July 6, 2017, 9:51 am

(Jul 6, 2017 09:39 AM)tra_extra Wrote: [\[CITE\]](#) After finding that block(s) what should i do?

I can't remove it(them) & keep comment(s) because i will lost functionality of my codes.

yes that's obvious
find a workaround.

d4rkP4n7h3r - July 6, 2017, 11:08 am

(Jul 6, 2017 09:35 AM)maldev0 Wrote: [\[CITE\]](#) Comment partial code blocks out and keep scanning until you find the code block which causes the detection(s). Find a workaround then.

This is the process. For future reference, usually when I am developing something that needs to remain in the dark I will scan as I code, saves me time having to comment out everything at the end. But when it comes to refuding, you'll just have to comment from top to bottom until you find the suspect line(s). If you're still struggling to FUD your program I can help you via jabber, just hmu. Best of luck! ?

Ninja - July 7, 2017, 6:56 am

From what I can tell, this is far over your head and you lack general problem solving skills. I suggest taking a step back and learn more.

tra_extra - July 7, 2017, 7:44 am

(Jul 7, 2017 06:56 AM)Ninja Wrote: [\[CITE\]](#) From what I can tell, this is far over your head and you lack general problem solving skills. I suggest taking a step back and learn more.

Thanks for the attention.

But step back where?

This thread is just for sharing all possible ways for FUD in coding.

How FUD an assembly without changing codes or add comments?

This is the question.

Here i am learning...

ForceJew - July 7, 2017, 10:02 am

(Jul 7, 2017 07:44 AM)tra_extra Wrote: [\[CITE\]](#) Thanks for the attention.

But step back where?

This thread is just for sharing all possible ways for FUD in coding.

How FUD an assembly without changing codes or add comments?

This is the question.

Here i am learning...

You don't remove u change ur way of doing things.

Ninja is right tho.

You need to learn about the language before going to crypters.

tra_extra - July 8, 2017, 10:48 am

Ok,

You mentioned on crypters.

How can i write a good one in c#?

Just show some sources about that.

ForceJew - July 8, 2017, 11:07 am

(Jul 8, 2017 10:48 AM)tra_extra Wrote: [\[CITE\]](#) Ok,

You mentioned on crypters.

How can i write a good one in c#?

Just show some sources about that.

Please this is making me cringe.

Do you know C#?

If you don't and ur "learning" it to make a crypter stop and make it ur hobby instead.

Cypical - July 8, 2017, 11:15 am

Learn C# properly first.

Making a crypter will come naturally after you know a lot about the language.

It is very common for noobs to try and code RAT/Crypter as soon as they've learned basic code.

ForceJew - July 8, 2017, 11:19 am

I also suggest u stay away from open source crypters.
Make ur own via non code details on how it works!

AmericanExpress - July 9, 2017, 9:55 am

The first thing you need to know is there there is a lot more to truly being FUD than just bypassing the static scanner. I suggest you invest time in actually learning how most modern security products work, I guarantee only a small majority mainly focus on static detection alone these days. FUD detection ratio on VirusTotal means absolutely nothing, honestly.

The second thing you need to remember is to stay away from just relying on a 'crypter'. Don't waste your money on the crap people post in the market place, hardly any of them actually know what they are doing and probably ripped most of it from open source code. Go ask them how they actually made their crypter or about run-time detection by AV products, I bet 90% of them won't even have a real answer to respond to you with.

You need to learn how different security products work because they don't all react to actions the same way. Make your functions into byte representation, check the AV installed and the copy the bytes which will not trigger the installed product to some memory and execute it. It is trial and error. You can use system calls to bypass UM interception but AVs also use kernel-mode via callbacks, kernel-mode patching (and in some scenarios, the fucking hyper-visor to bypass KPP). You need to code carefully and understand how different AV products work, you cannot just scrap together some shit and expect it to be FUD to every single AV product because you passed it through some crappy crypter being sold for \$30 on the market place.

/rant over

Good luck with studying!

xHeaven - July 9, 2017, 10:47 pm

Swap some lines, rewrite some lines (if you wrote the code, you can write that code on an other way), obfuscate the output etc..

tra_extra - July 9, 2017, 11:40 pm

(Jul 8, 2017 11:07 AM)FORC3FI3LD Wrote: [\[CITE\]](#) Please this is making me cringe.

Do you know C#?

If you don't and ur "learning" it to make a crypter stop and make it ur hobby instead.

Thanks people for the answers,

@FORC3FI3LD As i told you man i am c# developer & writing a crypter has nothing to do with my Skills.

Refer to AmericanExpress's answer & learn how people answer to a question.

I am here to gather all useful ideas & grab new things.

Cryptography & writing an obfuscator like smart assembly & etc in .net are in a different section of programming.

Also in this thread i asked about SandBox & no body here talk about that.

Nick (Name) - July 10, 2017, 12:11 am

I think you're lost buddy. I didn't have to ask around for "FUD code". You're leading yourself into the HF wannabe copy and paste scammers. If you fully understood how to work with memory and the basics of WinAPI I think you could do all this by yourself. You take your incompetence and try to make yourself look smart, stop it. No one wants more of the bullshit that already gets spread across the forum. About 60% of the developers here don't know what the hell they're doing but know the very basics of the language and how to copy and paste some nasty mess together, no structure or flow whatsoever. If you don't know C# I suggest grabbing a book, if you don't know anything about the Windows operating system, I suggest you grab a book. I bet you have a local bookstore nearby your city but you ignore the fact that it's there because everything can be accessed over the internet, while that's true, you can easily concentrate and focus on a book as it doesn't cause distractions than all the notifications and other shit on your computer.

tldr; read a book

tra_extra - July 10, 2017, 3:45 am

(Jul 10, 2017 12:11 AM)Nick (Name) Wrote: [\[CITE\]](#) I think you're lost buddy. I didn't have to ask around for "FUD code". You're leading yourself into the HF wannabe copy and paste scammers. If you fully understood how to work with memory and the basics of WinAPI I think you could do all this by yourself. You take your incompetence and try to make yourself look smart, stop it. No one wants more of the bullshit that already gets spread across the forum. About 60% of the developers here don't know what the hell they're doing but know the very basics of the language and how to copy and paste some nasty mess together, no structure or flow whatsoever. If you don't know C# I suggest grabbing a book, if you don't know anything about the Windows operating system, I suggest you grab a book. I bet you have a local bookstore nearby your city but you ignore the fact that it's there because everything can be accessed over the internet, while that's true, you can easily concentrate and focus on a book as it doesn't cause distractions than all the notifications and other shit on your computer.

tldr; read a book

I don't see any problem about copy paste if you know what are you doing!

Why are you so harsh?

Just open a Conversation around WinApi & explain more about that & keep your answer beautiful without any disrespect.

AmericanExpress - July 10, 2017, 4:10 am

(Jul 9, 2017 11:40 PM)tra_extra Wrote: [\[CITE\]](#) Also in this thread i asked about SandBox & no body here talk about that. A sandbox is very complicated to develop correctly. You will need to create a virtual environment which is based on the Host OS and then have your program executed within this information; you'll need to rely on native languages for such a project (e.g. work the Hyper-Visor from kernel-mode). I am not sure how other "protection" software rely on sandbox isolation as part of anti-reversing (they probably do not have a genuine, true "sandbox").

That being said, if you can successfully do it via hyper-visor implementation then you are in for a nice roller coaster ride since you'll be able to block access to your process, and not only this, but bypass KPP and rely on kernel-mode patching for your own environment! If you've ever wondered how Anti-Virus products develop a "secure browser" for sensitive browsing/banking, that is how.

(Jul 10, 2017 12:11 AM)Nick (Name) Wrote: [\[CITE\]](#) I think you're lost buddy. I didn't have to ask around for "FUD code". You're leading yourself into the HF wannabe copy and paste scammers. If you fully understood how to work with memory and the basics of WinAPI I think you could do all this by yourself. You take your incompetence and try to make yourself look smart, stop it. No one wants more of the bullshit that already gets spread across the forum. About 60% of the developers here don't know what the hell they're doing but know the very basics of the language and how to copy and

paste some nasty mess together, no structure or flow whatsoever. If you don't know C# I suggest grabbing a book, if you don't know anything about the Windows operating system, I suggest you grab a book. I bet you have a local bookstore nearby your city but you ignore the fact that it's there because everything can be accessed over the internet, while that's true, you can easily concentrate and focus on a book as it doesn't cause distractions than all the notifications and other shit on your computer.

tldr; read a bookI do not understand why you are speaking to him with this attitude... The point you mentioned about how OP should read a book is a good one because that can be incredibly beneficial, although there is no need to speak to him in the way you did. Even though I am not OP, reading your post does show a sense of hostility/aggressiveness.

You could have made a post to let him know he might benefit from reading a book or a few and then have linked him to some good ones you recommend which he may find educational. ?

xHeaven - July 10, 2017, 4:39 am

(Jul 10, 2017 03:45 AM)tra_extra Wrote: [\[CITE\]](#) I don't see any problem about copy paste if you know what are you doing!

Why are you so harsh?

Just open a Conversation around WinApi & explain more about that & keep your answer beautiful without any disrespect.

Dafuq are you talking about?

If you know what are you doing why should need to C+P? If you C+P the code, your program will be detected, because you'll use detected codes.

If you know how to code, why you can't simply change/recode the whole stuff and make it "FUD"? Almost everything new shit is "FUD", since they're just new, never used.

If you know what are you doing, why you asked this question?

Why you didn't do a proper research in the proper threads/sections?

The Google is your friend, the Wiki is your girlfriend, and the HF is.. the HF is idk, maybe your dad, but who cares.. Learn about the cryptography, learn about the resources, learn about the PE structure, learn about the memory, learn about the WinAPI, and learn how to write a code without begging for some C+P shit. There are a lot of tutorial/source/ebook on the internet, you can learn from them if you are a "visual coder" like me.

Btw, Nick wasn't (or weren't, fuck my english, I'm lost lmao) harsh, he was just honest. Take it and move on.

AmericanExpress - July 10, 2017, 4:56 am

^^ If OP was genuinely after a copy-paste then I regret what I said about Nick being too harsh and I agree. However if OP was just trying to obtain information about it so he can do it himself then what I said still stands.

tra_extra - July 10, 2017, 6:04 am

Some answers are just like BLO BLO BLO , Like a Geisha's (??) speech.

Just consider on Programming & Techniques...

+++++

A sandbox is a testing environment that isolates untested code changes and outright experimentation from the production environment or repository, in the context of software development including Web development and revision control.

Sandboxing protects "live" servers and their data, vetted source code distributions, and other collections of code, data and/or content, proprietary or public, from changes that could be damaging (regardless of the intent of the author of those changes) to a mission-critical system or which could

simply be difficult to revert. Sandboxes replicate at least the minimal functionality needed to accurately test the programs or other code under development (e.g. usage of the same environment variables as, or access to an identical database to that used by, the stable prior implementation intended to be modified; there are many other possibilities, as the specific functionality needs vary widely with the nature of the code and the application[s] for which it is intended).

The concept of the sandbox (sometimes also called a working directory, a test server or development server) is typically built into revision control software such as CVS and Subversion (SVN), in which developers "check out" a copy of the source code tree, or a branch thereof, to examine and work on. Only after the developer has (hopefully) fully tested the code changes in their own sandbox should the changes be checked back into and merged with the repository and thereby made available to other developers or end users of the software.

By further analogy, the term "sandbox" can also be applied in computing and networking to other temporary or indefinite isolation areas, such as security sandboxes and search engine sandboxes (both of which have highly specific meanings), that prevent incoming data from affecting a "live" system (or aspects thereof) unless/until defined requirements or criteria have been met.

+++++

Looking for sample codes if you are a developer!

If you don't know any thing about programming just don't bother yourself & don't answer here.

AmericanExpress - July 10, 2017, 6:22 am

(Jul 10, 2017 06:04 AM)tra_extra Wrote: [CITE](#) Some answers are just like BLO BLO BLO , Like a Geisha's (??) speech.

Just consider on Programming & Techniques...

+++++

A sandbox is a testing environment that isolates untested code changes and outright experimentation from the production environment or repository, in the context of software development including Web development and revision control.

Sandboxing protects "live" servers and their data, vetted source code distributions, and other collections of code, data and/or content, proprietary or public, from changes that could be damaging (regardless of the intent of the author of those changes) to a mission-critical system or which could simply be difficult to revert. Sandboxes replicate at least the minimal functionality needed to accurately test the programs or other code under development (e.g. usage of the same environment variables as, or access to an identical database to that used by, the stable prior implementation intended to be modified; there are many other possibilities, as the specific functionality needs vary widely with the nature of the code and the application[s] for which it is intended).

The concept of the sandbox (sometimes also called a working directory, a test server or development server) is typically built into revision control software such as CVS and Subversion (SVN), in which developers "check out" a copy of the source code tree, or a branch thereof, to examine and work on. Only after the developer has (hopefully) fully tested the code changes in their own sandbox should the changes be checked back into and merged with the repository and thereby made available to other developers or end users of the software.

By further analogy, the term "sandbox" can also be applied in computing and networking to other temporary or indefinite isolation areas, such as security sandboxes and search engine sandboxes (both of which have highly specific meanings), that prevent incoming data from affecting a "live" system (or aspects thereof) unless/until defined requirements or criteria have been met.

+++++

Looking for sample codes if you are a developer!

If you don't know any thing about programming just don't bother yourself & don't answer here. I'm aware of how a sandbox works, I've got experience with developing them. Not via the hyper-visor yet, but I'm getting there. (Have it ran under NT Authority\Anonymous logon like Sandboxie does and then prevent programs from accessing it). Hook & log APIs if necessary and rely on a KM driver to scan the process' memory and identify attempts of system call setup (e.g. copying bytes for an NTAPI function to newly allocated memory which contains the sysenter instruction, etc.).

If you're looking for sample codes on developing a sandbox in C# then you're having a laugh, but I don't mean this in a hostile way. AFAIK you cannot even do something like that in C#.NET alone, it wasn't built for security. You need to isolate it properly, not some half-assed copy pasted code. Even if someone can do something basic related to isolation in C# they are not going to post such a thing for free, even if it is in native they probably won't help you for free; there are open-source projects which use the hyper-visor but you have to learn how to use it yourself and you can't just c+p and claim it is yours, there is something called copyright protection and legal licenses.

Look into native programming in ASM, C and C++. If you want to make a real sandbox then invest time into kernel-mode device driver development and the hyper-visor (you'll need to support both Intel and AMD Systems.. Use Intel VT-x and AMD-v).

There is more to programming than developing a sandbox and you will need to be knowledgeable on A LOT more than just the .NET Framework and the Win32 API. More like the Native API, API hooking, system calls, memory protection, list goes on... If someone here doesn't know about it that doesn't mean they can't program, it is a complex project and not many people here even do low-level stuff such as sandbox isolation.

This is the worst place to ask for advice on something like a sandbox. We've already established most people here making crypters don't know anything, and general people who help out here focus on other things like normal software development, not security-focused on security development.

tra_extra - July 10, 2017, 7:46 am

@AmericanExpress, Thanks dude.

I accept your answer.

diiga - July 12, 2017, 7:06 am

here's an advice and never forget it dont scan in in virustotal -_-

ForceJew - July 12, 2017, 11:08 am

(Jul 12, 2017 07:06 AM)diiga Wrote: [\[CITE\]](#) here's an advice and never forget it dont scan in in virustotal -_-

A good crypter will stay FUD with VirusTotal too.

Ninja - July 12, 2017, 1:04 pm

(Jul 12, 2017 11:08 AM)FORC3FI3LD Wrote: [\[CITE\]](#) A good crypter will stay FUD with VirusTotal too. Thats not the point.

diiga - July 18, 2017, 4:54 pm

(Jul 12, 2017 11:08 AM)FORC3FI3LD Wrote: [\[CITE\]](#) A good crypter will stay FUD with VirusTotal too. even if it's an amazing crypter you shouldn't use VirusTotal it's like if you have a strong teeth that can break stones you could always break stone with them but if you keep it they will be broken eventually

ForceJew - July 18, 2017, 5:55 pm

(Jul 18, 2017 04:54 PM)diiga Wrote: [\[CITE\]](#) even if it's an amazing crypter you shouldn't use

VirusTotal it's like if you have a strong teeth that can break stones you could always break stone with them but if you keep it they will be broken eventually

Yea ofc you shouldn't

It's the same as using antibiotics for small headaches and shit.

Eventually it will develop a super bacteria and we will get fucked.

vorticalbox - July 24, 2017, 11:08 am

(Jul 6, 2017 09:50 AM)Maxim Wrote: [\[CITE\]](#) Here's a good thread for that topic:

<https://hackforums.net/showthread.php?tid=5639786>

don't these only scan the sample? doesn't check for things like run time detection ?

Don Genovese - July 24, 2017, 1:26 pm

(Jul 10, 2017 03:45 AM)tra_extra Wrote: [\[CITE\]](#) I don't see any problem about copy paste if you know what are you doing!

Why are you so harsh?

Just open a Conversation around WinApi & explain more about that & keep your answer beautiful without any disrespect.

You really do love your colours don't you.

Ninja - July 24, 2017, 6:48 pm

(Jul 18, 2017 05:55 PM)FORC3FI3LD Wrote: [\[CITE\]](#) Yea ofc you shouldn't

It's the same as using antibiotics for small headaches and shit.

Eventually it will develop a super bacteria and we will get fucked.

Headaches are usually not caused by bacteria though. And it is not a fitting analogy either.