

Forum:[Hack Forums](#)

Thread: [Payload Evasion Help: Meterpreter Payload+Shellter caught by defender behavior engine](#)

·CHESTER· - July 14, 2025, 8:20 pm

I am using Shellter to embed a meterpreter payload into an EXE. It doesn't get caught when statically checked, but it does get caught when I run it. It says WD catches it based on behavior. How do I bypass this?

DramaKing - July 14, 2025, 9:15 pm

I assume that you didn't pay for it (HF rules specifically forbid discussion of cracks/warez), and therefore you won't receive the upcoming version with enhanced runtime evasion. It's proprietary software, so you're stuck sifting through the Marketplace, looking for a crypter that's reasonably legit. Then you have to spread it in such a way that people will download and run it. Finally, you'll be able to hack people while jumping at every knock on your door.

·CHESTER· - July 15, 2025, 12:42 am

(Jul 14, 2025 09:15 PM)DramaKing Wrote: [\[CITE\]](#) I assume that you didn't pay for it (HF rules specifically forbid discussion of cracks/warez), and therefore you won't receive the upcoming version with enhanced runtime evasion. It's proprietary software, so you're stuck sifting through the Marketplace, looking for a crypter that's reasonably legit. Then you have to spread it in such a way that people will download and run it. Finally, you'll be able to hack people while jumping at every knock on your door.

I am using the free version of Shellter (not cracked version). But the main thing I am trying to achieve is to do everything for free. I don't want to buy rats or crypters. I want to use free and open source products or make it myself. But all the online guides tends to be outdated and its a random mixture of stuff. And when you come up against AV block, there is no guide for how to evade it.

DeathPenalty666 - July 15, 2025, 12:56 am

(Jul 15, 2025 12:42 AM)·CHESTER· Wrote: [\[CITE\]](#) I am using the free version of Shellter (not cracked version). But the main thing I am trying to achieve is to do everything for free. I don't want to buy rats or crypters. I want to use free and open source products or make it myself. But all the online guides tends to be outdated and its a random mixture of stuff. And when you come up against AV block, there is no guide for how to evade it.

if you head over kali linux, there is tools to create payload, rat, crypting and more for free. Like Byob, routersploit and more than could be great to make you something. Yeah defender will block any suspicious files or exploit that try to run malicious files. you can use batch or powershell script to bypass this, get the file crypted what is a must do to make it easier and or use exploit. with bat2exe, a bat to turn off defender and download it could work. with physical acces BADusd are terrible tool to do this.

·CHESTER· - July 15, 2025, 1:22 am

(Jul 15, 2025 12:56 AM)aralalala01 Wrote: [\[CITE\]](#) if you head over kali linux, there is tools to create payload, rat, crypting and more for free. Like Byob, routersploit and more than could be great to make you something. Yeah defender will block any suspicious files or exploit that try to run malicious files. you can use batch or powershell script to bypass this, get the file crypted what is a must do to make it easier and or use exploit. with bat2exe, a bat to turn off defender and download it could work. with physical acces BADusd are terrible tool to do this.

crypting is not going to get past runtime behavior detection, which is what the case is here

(Jul 15, 2025 12:49 AM)MarlboroMan Wrote: [\[CITE\]](#) Sigh...

<https://maldevacademy.com/>

holy shit can you stop shilling your dumb course? i read it the first time. now i am definitely not going to sign up for it because i know your scamming ass is involved.

DramaKing - July 15, 2025, 5:44 am

(Jul 15, 2025 12:42 AM)·CHESTER· Wrote: [\[CITE\]](#) I am using the free version of Shellter (not cracked version). But the main thing I am trying to achieve is to do everything for free. I don't want to buy rats or crypters. I want to use free and open source products or make it myself. But all the online guides tends to be outdated and its a random mixture of stuff. And when you come up against AV block, there is no guide for how to evade it.

Oh, okay. I saw the news about the leak and jumped to conclusions. Certainly the free version won't bypass behavioral/heuristic/AI detection. Open source crypters are good only for learning. Yeah, online guides are quickly outdated.

ttbr0 - July 16, 2025, 12:57 am

(Jul 16, 2025 12:35 AM)MarlboroMan Wrote: [\[CITE\]](#) Pretty much the only course that teaches skids (like you) the ropes off offensive security and helps you understand C/C++.

·CHESTER· - July 16, 2025, 1:52 am

(Jul 16, 2025 12:35 AM)MarlboroMan Wrote: [\[CITE\]](#) WTF. I'm not involved at ALL.

M4ldev happens to be one of the most legendary, beginner friendly courses. Pretty much the only course that teaches skids (like you) the ropes off offensive security and helps you understand C/C++.

This reply you just made shows how little input your putting in this. And btw calling me scammer is fucking stupid too, one glance at my contract stats would've learned you that too.

Just 1 hour of deep diving in the database would've expanded your horizon and knowledge.

<https://search.maldevacademy.com/search?q=evasion>

My advice: Stop making yourself loo

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

PS: Stop posting weird stuff like "Crypting doesn't get past runtime detections"

Why don't you go mind your own business. Stop replying to my threads.

·CHESTER· - July 16, 2025, 2:25 am

(Jul 16, 2025 02:02 AM)MarlboroMan Wrote: [\[CITE\]](#) Perhaps if you'd ask; I'd respect that.

You're making public threads with questions to which anyone including me can answer to.

The Acadamey [\(Click to View\)](#)

I'd also like to remind you that you need to follow The Academy's their rules when it comes to interacting with others on the forum if you're repping the group.

Shut the fuck up. No one asked for your opinion.

You are a dumb retard who doesn't read and just spams your scam course across every one of my threads. You don't ever read my issue or comment on that. You just make assumptions and start spamming your scam course. My thread about windows privilege escalation. Did you read it at all before spamming your dumb course? There is absolutely nothing on maldevscamademy that is about privilege escalation. Do you understand that there is no technique that will get you to privilege escalate on a fully updated windows 10 machine on factory settings, you dumb fuck? You couldn't hack your way out of a paper bag.

And also on maldevscamademy, half the course is like basic encrypting of payloads. If you ever read any of my posts, which you never do, you would know I have gone well past that long ago.

You have to sell your crypter for pennies because its dog shit, doesn't work, and no one wants it.

You are a dumb retard who needs to be banned of this site.

Jeep - July 16, 2025, 2:49 am

Instead of spamming your courses maybe show him some understanding rather promoting your shitty courses Marlboro

ttbr0 - July 16, 2025, 2:54 am

this is peak content

Jeep - July 16, 2025, 2:57 am

(Jul 16, 2025 02:51 AM)MarlboroMan Wrote: [\[CITE\]](#)

You guys have no idea how funny this is. The skids are putting it on their foreheads.

This is a legendary course.. which truly gives you the keys to offensive security.

Yet the skids (who clearly aren't invested at all) say this is my shitty scammy course? HILARIOUS. [censored] course are OK for starters but instead of promoting it many times since not everyone here will pay for the knowledge, you could help the OP with your knowledge rather than keep posting where to buy knowledge. He is asking for help not where to buy answers

Dystortion - July 16, 2025, 4:05 am

(Jul 16, 2025 03:05 AM)MarlboroMan Wrote: [\[CITE\]](#) Him reading the course able it trough cracking it is 200x times more useful than me trying to explain it. If you'd actually know you'd know.

What I don't get it why you guys don't bother taking the time to actually invest yourself in what a clearly more knowledgeable figure is telling you on the manner. Instead you respond out of your neck with completely self mockery (trust me saying m4ldev academy is mine and calling it scammy is one of the dumbest things you can state as an "hacker") without even fact checking yourself!

Even in the days of AI these skids don't bother to THINK.

What kind of immaturity is that?

This is pure quality lmao, MaldevAcademy produces some of the best content their is around Malware creation. And you, almighty [mention=5616027] should know that since you are the creator :PPP

Money- - July 16, 2025, 4:12 am

(Jul 16, 2025 12:35 AM)MarlboroMan Wrote: [\[CITE\]](#) WTF. I'm not involved at ALL.

M4ldev happens to be one of the most legendary, beginner friendly courses. Pretty much the only course that teaches skids (like you) the ropes off offensive security and helps you understand C/C++.

This reply you just made shows how little input your putting in this. And btw calling me scammer is fucking stupid too, one glance at my contract stats would've learned you that too.

Just 1 hour of deep diving in the database would've expanded your horizon and knowledge.

<https://search.maldevacademy.com/search?q=evasion>

My advice: Stop making yourself loo

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

PS: Stop posting weird stuff like "Crypting doesn't get past runtime detections"

hhahahaha this one made me chuckle. I legit thought this goofy name maldeva was actually yours lmaoooooooo. Mabolo.

7 - July 16, 2025, 4:17 am

This is a very explosive thread. But at least for once hackforums is arguing a about something intelligent.

Good advice MarlboroMan

·CHESTER· - July 16, 2025, 7:50 am

(Jul 16, 2025 03:05 AM)MarlboroMan Wrote: [\[CITE\]](#) Him reading the course able it trough cracking it is 200x times more useful than me trying to explain it. If you'd actually know you'd know.

What I don't get it why you guys don't bother taking the time to actually invest yourself in what a clearly more knowledgeable figure is telling you on the manner. Instead you respond out of your neck with completely self mockery (trust me saying m4ldev academy is mine and calling it scammy is one of the dumbest things you can state as an "hacker") without even fact checking yourself!

Even in the days of AI these skids don't bother to THINK.

What kind of immaturity is that?

tell me genius, which techniques on malscamacademy will get a meterpreter reverse shell past static and behaivoral windows defender? because it sure isn't aes encryption. and it isn't embedding it in an EXE either because that will get it caught behaivorally. so answer my question SPECIFICALLY: which techniques on malscamacademy will get a meterpreter reverse shell past static and behaivoral windows defender?

i know the answer: none of them

fucking moron speaking out of your ass and knowing nothing

·CHESTER· - July 16, 2025, 8:15 am

(Jul 16, 2025 08:11 AM)MarlboroMan Wrote: [\[CITE\]](#) Insane.. You still refuse to actually start learning..

<https://search.maldevacademy.com/updates>

Here you go chief. You've once again made a fool out of yourself..

This is peak content indeed ?

Once again, you didn't answer my question. Why don't you ever answer my question? Is it because you don't know the answer? That's exactly why.

Which techniques on malscamacademy will get a meterpreter reverse shell past static and behavioral windows defender?

ANSWER IT RETARD. I AM ASKING FOR NAMES OF TECHNIQUES. YOU CAN'T ANSWER IT CAUSE YOU DON'T KNOW SHIT.

7 - July 16, 2025, 8:19 am

(Jul 16, 2025 08:15 AM)·CHESTER· Wrote: [\[CITE\]](#) Once again, you didn't answer my question. Why don't you ever answer my question? Is it because you don't know the answer? That's exactly why.

Which techniques on malscamacademy will get a meterpreter reverse shell past static and behavioral windows defender?

ANSWER IT RETARD. I AM ASKING FOR NAMES OF TECHNIQUES. YOU CAN'T ANSWER IT CAUSE YOU DON'T KNOW SHIT.

Removed from The Academy for badly representing the Academy not respecting members who are trying to help or the rules of the Academy.

Not sure why this all got so aggressive but not under my name sorry.

@MarlboroMan@ is correct in everything he's suggesting if you want to learn to do this yourself free.

There is no free version of the solution you want.. you need to build it free=public=detected

No point in replying further or creating more drama that is said to all parties involved.

You wanted help, you were directed towards help and then attacked them for it.

You not encouraging users to try and assist you

·CHESTER· - July 16, 2025, 8:31 am

(Jul 16, 2025 08:19 AM)7 Wrote: [\[CITE\]](#) Removed from The Academy for badly representing the Academy not respecting members who are trying to help or the rules of the Academy.

Not sure why this all got so aggressive but not under my name sorry.

[mention=5616027] is correct in everything he's suggesting if you want to learn to do this yourself free.

There is no free version of the solution you want.. you need to build it free=public=detected

No point in replying further or creating more drama that is said to all parties involved.
You wanted help, you were directed towards help and then attacked them for it.

You not encouraging users to try and assist you

Waaa Waaa Waaa go kill yourself. You are a low IQ inbred loser with no life. Stop being a pedophile and talking to kids on a forum. You are loser with no family and spend all day in a forum with kids.

jcole - July 16, 2025, 8:36 am

(Jul 16, 2025 08:31 AM)·CHESTER· Wrote: [\[CITE\]](#) Waaa Waaa Waaa go kill yourself. You are a low IQ inbred loser with no life. Stop being a pedophile and talking to kids on a forum. You are loser with no family and spend all day in a forum with kids.

Don't act surprised when the community isn't interested in helping you with anything. Best of luck with your future endeavors cause your reputation is toast..

T3n - July 16, 2025, 8:37 am

(Jul 16, 2025 08:31 AM)·CHESTER· Wrote: [\[CITE\]](#) Waaa Waaa Waaa go kill yourself. You are a low IQ inbred loser with no life. Stop being a pedophile and talking to kids on a forum. You are loser with no family and spend all day in a forum with kids.

Calm down little guy, MarlboroMan told you to learn there's nothing wrong. You won't get spoonfed at every corner in life, just learn & STOP being so aggressive, nobody told u anything negative.

·CHESTER· - July 16, 2025, 8:50 am

(Jul 16, 2025 08:36 AM)jcole Wrote: [\[CITE\]](#) Don't act surprised when the community isn't interested in helping you with anything. Best of luck with your future endeavors cause your reputation is toast..
Go jump off a cliff you fucking inbred mongrel.

(Jul 16, 2025 08:37 AM)T3n Wrote: [\[CITE\]](#) Calm down little guy, MarlboroMan told you to learn there's nothing wrong. You won't get spoonfed at every corner in life, just learn & STOP being so aggressive, nobody told u anything negative.

I hope your whore mother gets gang raped by a pack of n1ggers with AIDS.

jcole - July 16, 2025, 9:04 am

(Jul 16, 2025 08:50 AM)·CHESTER· Wrote: [\[CITE\]](#) Go jump off a cliff you fucking inbred mongrel.

I hope your whore mother gets gang raped by a pack of n1ggers with AIDS.

Thanks for the kind words. I hope your day gets better. No point in escalating this more than it already has been.