

## Forum:[Hack Forums](#)

Thread: [c++ Crypter SC+exe, AES with CBC mode Polymorphic Encryption 100% FUD](#)

**SovietBastard** - August 19, 2024, 12:23 pm

how long will it take you to pull one out?

**James Clown** - August 19, 2024, 6:31 pm

(Aug 19, 2024 12:23 PM)SovietBastard Wrote: [\[CITE\]](#) how long will it take you to pull one out? Perhaps you could be more specific about what it is we should vote for.

The poll says: "How long". Are you asking how long it takes for us to pull something out and show how long it is?

That's disgusting. ^^

**SovietBastard** - August 19, 2024, 8:13 pm

(Aug 19, 2024 06:31 PM)James Clown Wrote: [\[CITE\]](#) Perhaps you could be more specific about what it is we should vote for.

The poll says: "How long". Are you asking how long it takes for us to pull something out and show how long it is?

That's disgusting. ^^

my friend, how long will it take u to write a FUD crypted... i dont expect many to answer less than 1 month

**ttbr0** - August 19, 2024, 8:23 pm

what conditions are we talking about? just static evasion or runtime? if runtime, what would be executed?

**SovietBastard** - August 19, 2024, 8:35 pm

(Aug 19, 2024 08:23 PM)ttbr0 Wrote: [\[CITE\]](#) what conditions are we talking about? just static evasion or runtime? if runtime, what would be executed?

conditions are those of a corp or big infra, runtime evasion, must perform basic standard data exfiltration, must be able to privesc, must keep persistence for at least 1/2 weeks, etc etc...

**ttbr0** - August 19, 2024, 9:15 pm

(Aug 19, 2024 08:35 PM)SovietBastard Wrote: [\[CITE\]](#) conditions are those of a corp or big infra, runtime evasion, must perform basic standard data exfiltration, must be able to privesc, must keep persistence for at least 1/2 weeks, etc etc...

if you say corp or big infra, does that imply edr? if so, does that then imply a soc/blue team? those circumstances are far beyond the scope of what a crypter does. evasion of human analysts is the job of the operator. i dont agree on some of these requirements being the job of a crypter.

**SovietBastard** - August 20, 2024, 7:20 am

(Aug 19, 2024 09:15 PM)ttbr0 Wrote: [\[CITE\]](#) if you say corp or big infra, does that imply edr? if so, does that then imply a soc/blue team? those circumstances are far beyond the scope of what a crypter does. evasion of human analysts is the job of the operator. i dont agree on some of these requirements being the job of a crypter.

HOW LONG WILL IT TAKE YOU TO WRITE 100% FUD CRYPTER? i don't care what is being executed, that's the malware job, what im asking is CAN YOU WRITE 100% FUD CRYPTER? either YES or NO, if YES, HOW LONG WILL IT TAKE YOU?

(Aug 19, 2024 08:23 PM)ttbr0 Wrote: [\[CITE\]](#) what conditions are we talking about? just static evasion or runtime? if runtime, what would be executed?

again, it doesn't matter what is being executed, that is the job of the malware, not the crypter, the crypter only has one role, crypt the malware, so the above requirements do not matter in the context, the evasion or execution is not the crypter field... do crypters really execute payloads? not really... ..

**dobroy\_000** - August 21, 2024, 2:54 am

i would never be able to write a crypter, kind of too complex i guess

**ttbr0** - August 21, 2024, 4:15 am

(Aug 20, 2024 07:20 AM)SovietBastard Wrote: [\[CITE\]](#) HOW LONG WILL IT TAKE YOU TO WRITE 100% FUD CRYPTER? i don't care what is being executed, that's the malware job, what im asking is CAN YOU WRITE 100% FUD CRYPTER? either YES or NO, if YES, HOW LONG WILL IT TAKE YOU?

again, it doesn't matter what is being executed, that is the job of the malware, not the crypter, the crypter only has one role, crypt the malware, so the above requirements do not matter in the context, the evasion or execution is not the crypter field... do crypters really execute payloads? not really... ..

youre attempting to tie the meaning of "crypter fud" with actions that will raise detections that are beyond the responsibilities of the crypter. imo the crypter is only supposed to protect the malware from any detection until the first few moments of execution. beyond that, any action is the responsibility of the payload and the operator. any further features in the stub is counter intuitive and unnecessary, even potentially detrimental because it may bring about undesirable side effects that may increase detection. keep it simple and disposable. the crypter is not meant to facilitate data exfiltration, that is nonsensical.

that being said, a simple crypter is relatively simple to develop but that depends on how fast you write code and how well you want it to scale. its simple to write a quick and dirty crypter within a week but one that supports multiple file types with unique metamorphed stubs on every crypt with infra that has a pipeline to automatically deploy machines with av to test could take many many months to engineer and develop.

**super\_sayan** - August 21, 2024, 4:46 am

(Aug 21, 2024 04:15 AM)ttbr0 Wrote: [\[CITE\]](#) youre attempting to tie the meaning of "crypter fud" with actions that will raise detections that are beyond the responsibilities of the crypter. imo the crypter is only supposed to protect the malware from any detection until the first few moments of execution. beyond that, any action is the responsibility of the payload and the operator. any further features in the stub is counter intuitive and unnecessary, even potentially detrimental because it may bring about undesirable side effects that may increase detection. keep it simple and disposable. the crypter is not meant to facilitate data exfiltration, that is nonsensical.

that being said, a simple crypter is relatively simple to develop but that depends on how fast you write code and how well you want it to scale. its simple to write a quick and dirty crypter within a week but one that supports multiple file types with unique metamorphed stubs on every crypt with infra that has a pipeline to automatically deploy machines with av to test could take many many months to engineer and develop.

LOL, I must emphasize that your recent response appears to sidestep the primary objective of the discussion, which is to thoroughly analyze the core issue at hand. In order to facilitate a constructive dialogue, it is essential to address the specific points raised rather than redirecting the conversation towards peripheral themes, this approach not only enhances clarity but also fosters a more productive exchange of ideas, allowing us to reach a consensus or actionable solutions more efficiently, i REALLY encourage you to revisit the salient aspects of the topic for a more substantive interaction moving forward. You did not answer to OP question btw...

ttbr0 - August 21, 2024, 5:09 am

(Aug 21, 2024 04:46 AM)super\_sayan Wrote: [\[CITE\]](#) LOL, I must emphasize that your recent response appears to sidestep the primary objective of the discussion, which is to thoroughly analyze the core issue at hand. In order to facilitate a constructive dialogue, it is essential to address the specific points raised rather than redirecting the conversation towards peripheral themes, this approach not only enhances clarity but also fosters a more productive exchange of ideas, allowing us to reach a consensus or actionable solutions more efficiently, i REALLY encourage you to revisit the salient aspects of the topic for a more substantive interaction moving forward. You did not answer to OP question btw...

its important to clarify and understand all details for a task before knowing what specifics are needed to implement a particular tool and its features. what i have deemed as critical details i have asked for elaboration yet there seems to be disagreements about what constitutes as important pushes back on the conclusions i can make to give an answer, which i have given as an estimate. yet strangely enough you are here using fluff statements and words to put me on the spot to get me to give an answer but not providing your own? so i am here to return your favor, why dont you give us an answer to the question?

super\_sayan - August 21, 2024, 5:50 am

(Aug 21, 2024 05:09 AM)ttbr0 Wrote: [\[CITE\]](#) its important to clarify and understand all details for a task before knowing what specifics are needed to implement a particular tool and its features. what i have deemed as critical details i have asked for elaboration yet there seems to be disagreements about what constitutes as important pushes back on the conclusions i can make to give an answer, which i have given as an estimate. yet strangely enough you are here using fluff statements and words to put me on the spot to get me to give an answer but not providing your own? so i am here to return your favor, why dont you give us an answer to the question?

?? LMAO i dying ... so funny seeing you trying to correct or collide with SB ?, do you even know who the guy is? holy mother, im sure you don't.... if he used the real nickname or just the group is member of, believe me you would stop arguing anything comes out of his mouth and will make you raise your eyebrows over your head... and no, i don't know about crypters, but if you write in PM to SB, maybe he could be generous and teach you something... my answer to SB question is "+1 month" because i don't know much about crypters, see? at least i got a response back, wbu?

dobroy\_000 - August 21, 2024, 6:12 am

(Aug 21, 2024 04:15 AM)ttbr0 Wrote: [\[CITE\]](#) youre attempting to tie the meaning of "crypter fud" with actions that will raise detections that are beyond the responsibilities of the crypter. imo the crypter is only supposed to protect the malware from any detection until the first few moments of execution. beyond that, any action is the responsibility of the payload and the operator. any further features in the stub is counter intuitive and unnecessary, even potentially detrimental because it may bring about undesirable side effects that may increase detection. keep it simple and disposable. the crypter is not meant to facilitate data exfiltration, that is nonsensical.

that being said, a simple crypter is relatively simple to develop but that depends on how fast you write code and how well you want it to scale. its simple to write a quick and dirty crypter within a week but one that supports multiple file types with unique metamorphed stubs on every crypt with infra that has a pipeline to automatically deploy machines with av to test could take many many

months to engineer and develop.

??? my god, that is cringe AF, i will tell you a secret, someone here is making fun of you and you r playing very bad... first rule of a good BH? please answer me this question, what is the first rule for a BH? LOL... pay attention to OP question semantics, he "almost" made it clear, you're not very good at semantic analysis do you?

**SovietBastard** - August 23, 2024, 4:37 am

(Aug 22, 2024 10:35 PM)blyat1337 Wrote: [\[CITE\]](#) So much yapping. I already have my full PIC crypter with anti emulation/VM and undetected execution method on every EDR possible.

Took me 1 week of 2 hours a day.

The polyengine took also 1 week.

Overall, it produces 100% unique code every single time.

what do you think about polymorphic vs metamorphic? polymorphic transforms the code so bypasses signature detection, metamorphic bypasses both signature+behavior detection, i feel like building a polymorphic crypter is not easy task, but metamorphic is really complex, what do you think? you seem to be knowledgeable and reasonable guy

**SovietBastard** - August 23, 2024, 8:13 am

(Aug 23, 2024 06:06 AM)blyat1337 Wrote: [\[CITE\]](#) Let me start by telling you something straightforward: with crypting, you want to perform less work in order to get more done. Clearly, this isn't functional in the \$20/month or \$50/month crypters that individuals are attempting to sell here, as those involve "manually" eliminating detections.

For months on end, no one is going to spend 6-7 hours a day by hand "removing" portions of the code in order to "bypass" Defender just to receive \$60 for a lifetime license.

Ninety percent of crypters scam or plan to scam after working for a month or two, or they just keep milking a dead cow by selling highly detectable software, because manual is DEAD and simply too hard to maintain.

AI engines are currently the largest problem; Defender is a prime example. What's worse is that every file that is executed or dropped to disk is instantly transmitted to their labs where it is automatically analyzed, categorized, and flagged by DEFENDER (If it is known malware) - This can happen as fast as 10 minutes, chrome flagging is even faster, 2-5 minutes. Because of its strength, the AI engine will be able to identify and flag any additional occurrences of the same stub and they will be categorized as the same group.

Therefore, it only takes one file execution to FLAG a "base" stub and flag any subsequent iterations as well. The AI takes into consideration a lot of factors: Resources, Import hashing, entropy and a lot more.

So why engage in a losing war? Why not put AI to use for your own benefit? Why not host your PIC loader on actual files/ real files? The DEFENDER/other AV database will flag it as "legit" because it is in their database of "good samples" /downloaded samples.

Such files are infinite, and if you use a good Poly engine, you won't even need to work for longer than five minutes.. Morphing PIC shellcode is a lot simpler then morphing a whole PE, and even worse, morphing a whole PE will bring a lot of anomalies which you want to avoid, AI eats them for breakfast.

That is my 2cents.

I don't bother with metamorphic myself, because it is too much for such a simple task which can be

achieved by what I specified, as far as runtime it is not the job of a crypter.

If the coder of your malware is an idiot, you will be detected.

You can look at some great malware writers like rhadamanthys, lummac2, xloader. Such software does not require a meta engine for runtime, simply because it was written with evasion in mind.

Heck if you are a real threat actor, you will never use premade software, you write it yourself or pay big \$\$ for others to do it for you.

People like that are not here, and I am... just a, visitor)

thank you for the reply, yeah, almost always they pull out they're own shit, it is better of course! as i said, you're one of the few if not the only one who sounds knowledgeable here

(Aug 23, 2024 06:06 AM)blyat1337 Wrote: [\[CITE\]](#) Let me start by telling you something straightforward: with crypting, you want to perform less work in order to get more done. Clearly, this isn't functional in the \$20/month or \$50/month crypters that individuals are attempting to sell here, as those involve "manually" eliminating detections.

For months on end, no one is going to spend 6-7 hours a day by hand "removing" portions of the code in order to "bypass" Defender just to receive \$60 for a lifetime license.

Ninety percent of crypters scam or plan to scam after working for a month or two, or they just keep milking a dead cow by selling highly detectable software, because manual is DEAD and simply too hard to maintain.

AI engines are currently the largest problem; Defender is a prime example. What's worse is that every file that is executed or dropped to disk is instantly transmitted to their labs where it is automatically analyzed, categorized, and flagged by DEFENDER (If it is known malware) - This can happen as fast as 10 minutes, chrome flagging is even faster, 2-5 minutes. Because of its strength, the AI engine will be able to identify and flag any additional occurrences of the same stub and they will be categorized as the same group.

Therefore, it only takes one file execution to FLAG a "base" stub and flag any subsequent iterations as well. The AI takes into consideration a lot of factors: Resources, Import hashing, entropy and a lot more. Just imagine how strong it is, it has billions of samples, millions new every day.

So why engage in a losing war? Why not put AI to use for your own benefit? Why not host your PIC loader on actual files/ real files? The DEFENDER/other AV database will flag it as "legit" because it is in their database of "good samples" /downloaded samples.

Such files are infinite, and if you use a good Poly engine, you won't even need to work for longer than five minutes.. Morphing PIC shellcode is a lot simpler then morphing a whole PE, and even worse, morphing a whole PE will bring a lot of anomalies which you want to avoid, AI eats them for breakfast.

That is my 2cents.

I don't bother with metamorphic myself, because it is too much for such a simple task which can be achieved by what I specified, as far as runtime it is not the job of a crypter.

If the coder of your malware is an idiot, you will be detected. The job of the crypter is to be a PERFECTLY RUNTIME FUD EXECUTOR, THAT IS ALL. Execute the payload, what happens after, is issue of malware.

You can look at some great malware writers like rhadamanthys, lummac2, xloader. Such software does not require a meta engine for runtime, simply because it was written with evasion in mind.

Heck if you are a real threat actor, you will never use premade software, you write it yourself or pay big \$\$ for others to do it for you.

People like that are not here, and I am... just a, visitor)

i tried to text u in PM but requires upgrade, what a weird thing, btw... i was about to ask u if u r on exploitdotin

**Informant** - August 24, 2024, 5:51 am

(Aug 23, 2024 08:13 AM)SovietBastard Wrote: [\[CITE\]](#) thank you for the reply, yeah, almost always they pull out they're own shit, it is better of course! as i said, you're one of the few if not the only one who sounds knowledgeable here

i tried to text u in PM but requires upgrade, what a weird thing, btw... i was about to ask u if u r on exploitdotin

You say "i tried to text u in PM but requires upgrade, what a weird thing, btw... i was about to ask u if u r on exploitdotin".

You are talking to your self, scammer lmao.

AND NO - ITS NOT WIERD TO REQUIRE UPGRADE TO TEXT OTHER MEMBER ON PM.

It is for prevent scam, like you and "your friend" account name blyat1337 did to me on Telegram.

I will report you to the owner of Hackforum for using many account on Hackforum and scamming and you also do this from russian forum (exploit.in) and you said this yourself).

I will now reveal for the owner of Hackforum [Omniscient](#) to know that this members are the same member:

blyat1337 = SovietBastard

He is also on exploit.in and scam people there.

I hope that this will save other victims of the scammer blyat1337 = SovietBastard.

Nahui blyat1337 and SovietBastard (It mean fuck off in russian basically).

Thank you.

**b0r\_ealis** - August 24, 2024, 7:38 am

(Aug 24, 2024 06:27 AM)blyat1337 Wrote: [\[CITE\]](#) Being schizophrenic is a mad disease. I do not need to scam anyone, I do not sell anything here nor on exploit. I am just a simple man who likes to speak wise words.

You can't blame me to be someone else just because I am russian, lmao.

People tend to be schizo when they don't understand truer words, to which have never been spoken before. Don't indulge in it, I appreciate the insight that may help the others out there.

**SovietBastard** - August 24, 2024, 8:52 am

(Aug 24, 2024 05:51 AM)Informant Wrote: [\[CITE\]](#) You say "i tried to text u in PM but requires upgrade, what a weird thing, btw... i was about to ask u if u r on exploitdotin".

You are talking to your self, scammer lmao.

AND NO - ITS NOT WIERD TO REQUIRE UPGRADE TO TEXT OTHER MEMBER ON PM.

It is for prevent scam, like you and "your friend" account name blyat1337 did to me on Telegram.

I will report you to the owner of Hackforum for using many account on Hackforum and scamming and you also do this from russian forum (exploit.in) and you said this yourself).

I will now reveal for the owner of Hackforum [Omniscient](#) to know that this members are the same member:

blyat1337 = SovietBastard

He is also on exploit.in and scam people there.

I hope that this will save other victims of the scammer blyat1337 = SovietBastard.

Nahui blyat1337 and SovietBastard (It mean fuck off in russian basically).

Thank you.

.... sniffing crack ?