

Forum:[Hack Forums](#)

Thread: [Meta Engine?](#)

Praet0rian - February 17, 2017, 12:05 pm

I'm curious. how much would people be ready to pay for a true metamorphic engine?
what about a polymorphic engine?

Codefuser - February 17, 2017, 11:01 pm

You won't be able to sell this on HF. Get on other forums like exploit.in.

HF's userbase is 99% noobs who have no idea how to use a crypter and will not pay for something that advanced.

GabrielAtanasov - February 17, 2017, 11:03 pm

I'm new here and I have question ?? what does mean polymorphic engine?

Codefuser - February 17, 2017, 11:17 pm

(Feb 18, 2017 12:03 AM)GabrielAtanasov Wrote: [\[CITE\]](#) I'm new here and I have question ?? what does mean polymorphic engine?

Exactly my point OP. 99.9% of HF are like this.

GabrielAtanasov - February 17, 2017, 11:18 pm

(Feb 18, 2017 12:17 AM)Codefuser Wrote: [\[CITE\]](#) Exactly my point OP. 99.9% of HF are like this.
You sad me man ?

Russel_Novagan - February 17, 2017, 11:31 pm

(Feb 18, 2017 12:18 AM)GabrielAtanasov Wrote: [\[CITE\]](#) You sad me man ?

I can be unclear on this, so sorry in advance. Polymorphic engine means that the calls, classes and metadata of your file will randomize automatically on each crypt. This will result longer FUD times because it's a new programm basically. Metamorphic engine embeds special machine code into your file without interrupting it's work. Software like this is very expensive and hard to find.

GabrielAtanasov - February 17, 2017, 11:51 pm

(Feb 18, 2017 12:31 AM)Russel_Novagan Wrote: [\[CITE\]](#) I can be unclear on this, so sorry in advance. Polymorphic engine means that the calls, classes and metadata of your file will randomize automatically on each crypt. This will result longer FUD times because it's a new programm basically. Metamorphic engine embeds special machine code into your file without interrupting it's work. Software like this is very expensive and hard to find.

Thank you so much. It's look very interesting.

Praet0rian - February 18, 2017, 1:42 am

(Feb 18, 2017 12:31 AM)Russel_Novagan Wrote: [\[CITE\]](#) I can be unclear on this, so sorry in advance. Polymorphic engine means that the calls, classes and metadata of your file will randomize automatically on each crypt. This will result longer FUD times because it's a new programm basically. Metamorphic engine embeds special machine code into your file without interrupting it's work. Software like this is very expensive and hard to find.

Metamorphic engines go far beyond simply adding junk code, they can also modify the code in a

way that the code is different, but has the same output, here is a basic example in assembly:

instead of doing this:

Code mov eax, 5a metamorphic engine would modify it so that

Code mov eax, 2

add eax 3at the end of the modification, eax still has 5, at the end, but the way it got it is different.

the problem is that with playing around with code you might fuck it up at any point, so you must account for it all and also when you are adding code it will also be required to modify the PE header[for windows], in order to account for these changes

overall it requires mastery of the PE format, mastery over assembly, and you will need some serious algo skills, you can only imagine how complicated this can be, yet so powerful.

Codefuser - February 18, 2017, 5:46 am

(Feb 18, 2017 02:42 AM)Praet0rian Wrote: [\[CITE\]](#) Metamorphic engines go far beyond simply adding junk code, they can also modify the code in a way that the code is different, but has the same output, here is a basic example in assembly:

instead of doing this:

Code mov eax, 5a metamorphic engine would modify it so that

Code mov eax, 2

add eax 3at the end of the modification, eax still has 5, at the end, but the way it got it is different.

the problem is that with playing around with code you might fuck it up at any point, so you must account for it all and also when you are adding code it will also be required to modify the PE header[for windows], in order to account for these changes

overall it requires mastery of the PE format, mastery over assembly, and you will need some serious algo skills, you can only imagine how complicated this can be, yet so powerful.

Which is why HF is not the place for this. It is simply above HF's level.

Praet0rian - February 18, 2017, 10:04 am

(Feb 18, 2017 06:46 AM)Codefuser Wrote: [\[CITE\]](#) Which is why HF is not the place for this. It is simply above HF's level.

Yeah well, I don't know Russian Imao

Not that I could make a metamorphic engine in the near future anyway

I was merely curious on how much it would cost

chvrn - February 18, 2017, 1:08 pm

To add: the distinction between a polymorphic engine and a metamorphic one is that the latter is general enough to morph its own code.

(Feb 18, 2017 02:42 AM)Praet0rian Wrote: [\[CITE\]](#) Code mov eax, 5a metamorphic engine would modify it so that

Code mov eax, 2

add eax 3the problem is that with playing around with code you might fuck it up at any point, so you must account for it allPretty good example given that the latter sets flags conditionally

Codefuser - February 18, 2017, 9:57 pm

(Feb 18, 2017 11:04 AM)Praet0rian Wrote: [\[CITE\]](#) Yeah well, I don't know Russian Imao

Not that I could make a metamorphic engine in the near future anyway

I was merely curious on how much it would cost

Pay \$100 to the owner and you can get in.

ezz

Praet0rian - February 20, 2017, 8:32 am

(Feb 18, 2017 02:08 PM)chvrn Wrote: [\[CITE\]](#) To add: the distinction between a polymorphic engine and a metamorphic one is that the latter is general enough to morph its own code.

Pretty good example given that the latter sets flags conditionally
yep,, I'm not too good at assembly, but I reckon if you pushof before and popf after it can help,
also saving the flags register manually could work too, but even then, very problematic.
also, i believe my example was polymorphic, rather than metamorphic, based on wikipedia anyway