

Forum:[Hack Forums](#)

Thread: [Convinced All The Crypters Here are Garbage](#)

Non Serviam - January 30, 2018, 4:56 pm

I have literally bought almost all of the crypters on hackforums,

The only one that even made halfass decent crypts was dataprotector but even now at this time it is garbage.

There is literally no crypter on this sub forum I have found that is actually worth paying for.

Why don't one of you programmers be smart about this shit and make a HIGH QUALITY NATIVE crypter with ACTUAL RUNTIME UD and sell it for \$400 + per spot.

Stop making this \$15 - \$50 per license garbage

its really trash and all this shit is basically a scam....

Sheeple - January 30, 2018, 4:59 pm

Because a lot of people will buy a 10\$ crypter vs a 400\$ one.

What do you use the crypters here for anyways?

Non Serviam - January 30, 2018, 5:01 pm

(Jan 30, 2018 05:59 PM)Sheeple Wrote: [\[CITE\]](#) Because a lot of people will buy a 10\$ crypter vs a 400\$ one.

What do you use the crypters here for anyways?

Private use, targeted machines

no spreading

to bad no programmer doesn't see the honeypot of money opportunity here

UpTheCrust - January 30, 2018, 5:03 pm

I've definitely seen some of these advertised on here. The sales threads tend to get buried though because like Sheeple said, people prefer cheap crypters even if they have shorter FUD times

Peace Security - January 30, 2018, 5:09 pm

The reason that most people prefer paying less is because 99% of crypters say "Weeks FUD" or "Long FUD" time and really it's either never FUD to begin with and or it's FUD and detection Rate is within 24 hours

I will give Credit to DataProtector because I have had a file go FUD for 1 week before any detection's

Fulya Donmez - January 30, 2018, 11:30 pm

If i may ask what Rat or Botnet are you using the crypter for?

SIM-2223238 - January 30, 2018, 11:33 pm

Because sellers want mass marketing, not your personal skid developer. Just get someone to code you one for scratch or pay \$150 per crypt on exploit(site)

Flacon - January 31, 2018, 3:55 am

get a good malware first then you might get a good crypter i can not suggest any cause pretty much all malware i know is garbage

Peace Security - January 31, 2018, 4:50 am

(Jan 31, 2018 04:55 AM)Flacon Wrote: [\[CITE\]](#) get a good malware first then you might get a good crypter i can not suggest any cause pretty much all malware i know is garbage
I wouldn't say all malware, most people know about smoke loader and it's still one of the best around ?

AlexCanvas - January 31, 2018, 6:13 am

(Jan 30, 2018 06:01 PM)Blanc0 Wrote: [\[CITE\]](#) to bad no programmer doesn't see the honeypot of money opportunity here
Do you have any idea how annoying it is to deal with customers on HF?

h40xer - January 31, 2018, 8:19 am

Im using Flowcrypter and its doing the job, you can buy a private stub if you expect run times to be good.

Manks - January 31, 2018, 8:22 am

(Jan 31, 2018 07:13 AM)AlexCanvas Wrote: [\[CITE\]](#) Do you have any idea how annoying it is to deal with customers on HF?
A customer here, is also a customer somewhere else. If you can't deal with HF users, you're gonna have a hard time selling anything.

HotTunaCanSandiwch - January 31, 2018, 8:50 am

bro ofc you get garbage, you pay for what you eat,
you cant expect to buy a 15 dollar crypter or 30 dollar crypter and expect FUD.
you want it to be fully undetected? get ready to spend atleast 150 dollars a month (if you are lucky)
you are buying public crypters that get sold to cats and dogs, and end up getting the stub detected. go private or go home

mehtevs - January 31, 2018, 9:05 am

(Jan 31, 2018 09:50 AM)HotTunaCanSandiwch Wrote: [\[CITE\]](#) bro ofc you get garbage, you pay for what you eat,
you cant expect to buy a 15 dollar crypter or 30 dollar crypter and expect FUD.
you want it to be fully undetected? get ready to spend atleast 150 dollars a month (if you are lucky)
you are buying public crypters that get sold to cats and dogs, and end up getting the stub detected. go private or go home
you miss spelled indians and nigerians

inyourmemory - January 31, 2018, 10:47 am

(Jan 31, 2018 05:50 AM)?Monster Energy Wrote: [\[CITE\]](#) I wouldn't say all malware, most people know about smoke loader and it's still one of the best around ?
SmokeLoader isnt even that good lmao, its one of the cheapest bots theres around

Fulya Donmez - January 31, 2018, 12:17 pm

(Jan 31, 2018 11:47 AM)Win64Worm Wrote: [\[CITE\]](#) SmokeLoader isnt even that good lmao, its one of the cheapest bots theres around

Which one is better than smoke?

05317832892 - January 31, 2018, 1:59 pm

Problem is most of the shit on here is C&P.

mehtevas, AriesCoder and Friedrich Nietzsche are legit. The rest is just C# public RunPE bs.

It's easy to tell if a crypter is shit, just look at their sales thread, if its proxy sell horse shit, they will promote their fancy "vbc" or "runasm" injection or their file pumper (like why the fuck is this even a thing? you want to make your file small with low entropy and normalised sections, not huge with 90% .data 7.9 entropy), or their startup methods.

Real coders promote the shit that matters, syscall extraction, stub size, API bypasses, heuristics.

Marriot170 - February 1, 2018, 4:38 pm

(Jan 31, 2018 02:59 PM)ROOTED Wrote: [\[CITE\]](#) Problem is most of the shit on here is C&P.

mehtevas, AriesCoder and Friedrich Nietzsche are legit. The rest is just C# public RunPE bs.

It's easy to tell if a crypter is shit, just look at their sales thread, if its proxy sell horse shit, they will promote their fancy "vbc" or "runasm" injection or their file pumper (like why the fuck is this even a thing? you want to make your file small with low entropy and normalised sections, not huge with 90% .data 7.9 entropy), or their startup methods.

Real coders promote the shit that matters, syscall extraction, stub size, API bypasses, heuristics.
Thank you for existing and for saying the right things.
This post should be pinned for view in the cryptography section..

Almost every other .NET crypter here is based off Aeonhack's runPE.
Then they use ConfuserEx and call it 'ADVANCED USG'.

05317832892 - February 2, 2018, 7:55 am

(Feb 1, 2018 05:38 PM)Marriot170 Wrote: [\[CITE\]](#) Thank you for existing and for saying the right things.

This post should be pinned for view in the cryptography section..

Almost every other .NET crypter here is based off Aeonhack's runPE.
Then they use ConfuserEx and call it 'ADVANCED USG'.
Lol my crypter is 100% asm so I can do a lot of black magic.

It uses sysenter on native x32 machines and transition on x64 to evade all ring-3 hooks, doesn't map ntdll or rely on the in memory one provided by winloader.

The engine is about 100 asm instructions, very small. It's stored xor'd in .data. I just jump to it once the pre req has completed. It's not position independent though because it relies on known offsets.

Most shitty crypters will AES the binary or use some other high entropy blaintent bs, because I'm working with asm I can encode the PE in the junk asm operand values, for example:

Code mov eax,0
Will be encoded as

Code \xB8 \x00 \x00 \x00 \x00

However if I want to store a PE file, I split it up into dwords (4 byte sections) and xor each against a fixed key, then use the value as the operand for a junk code instruction.

Examples of instructions that can work for this are as follows:

- JMP (and it's variations)
- CALL
- MOV (and some of its variations)
- ADD
- SUB
- OR
- AND
- PUSH

Most of them have a ratio of 1:4 so only around 25% size increase in return for valid normal (ish) entropy heuristically correct file. It also doubles up as junk code that's never executed.

One odd thing I have noticed in using this technique though is that there's no limitations on jmp and call instructions, usually they should only point to somewhere in the range of (PE Base address + Total virtual size) however AVs have no problem with a series of hard coded jumps to high/low memory locations.

My stub also has self modifying code within .text, it calls virtual protect against the base of .text to allow modifications, it then modified the values in the xor decryption routines.

There are 2 decryption routines, 1 for the engine, 1 for the payload PE file. These are fairly obvious if you look disassemble however the self modifying code will modify the xor values. If you look at the binary in IDA, you can see the decryption routine, however at run-time, the "hardcoded" key used to decode is altered via self modification from a different section of code. This causes confusion for an beginner analyst as he will see only 1 xref to the engine code but the xor doesn't actually work because the key is invalid.

Oh and there's a shit ton of anti-debug / anti-automation / anti-sandbox. All under 15kb, FUD.

I've basically just given all the retards on here a blueprint for a good crypter, too bad none of them know a language other than vb.net

0x0F0C - February 2, 2018, 8:37 am

(Feb 2, 2018 08:55 AM)ROOTED Wrote: [\[CITE\]](#) However if I want to store a PE file, I split it up into dwords (4 byte sections) and xor each against a fixed key, then use the value as the operand for a junk code instruction.

Examples of instructions that can work for this are as follows:

- JMP (and it's variations)
- CALL
- MOV (and some of its variations)
- ADD
- SUB
- OR
- AND
- PUSH

Great Work ! , but some AVs (like Comodo / Kaspersky / Avira /Avast /Bitdefender) disassemble the code and check if it's junk code .

they check if you assign value to register and dont use them , check validity of MOV/JMP/Call

Addresses

And you should have full code disassembler in your stub right ?

05317832892 - February 2, 2018, 9:14 am

(Feb 2, 2018 09:37 AM)ivdz Wrote: [\[CITE\]](#) Great Work ! , but some AVs (like Comodo / Kaspersky / Avira /Avast /Bitdefender) disassemble the code and check if it's junk code .

they check if you assign value to register and dont use them , check validity of MOV/JMP/Call

Addresses

And you should have full code disassembler in your stub right ?

The last part is incorrect in my experience, when I have junk code that jumps to fake addresses it doesn't cause detection.

I encode it like

```
mov eax,BYTES
xor eax,BYTES
mov BYTES, eax
add [BYTES],eax
```

So it is junk code however interlaced references make it look fine.

Code global _start

```
section .text
```

```
_start:
```

```
    call _cabbage
```

```
_cabbage:
```

```
    mov  eax,0
```

Then I opened up in hxd and changed the call to an invalid address

<https://www.virustotal.com/#/file/e57c8d042f467ea92332d42e7819488dbefc272b9338173ad3010a542d063484/detection>

2/65, neither of those detections are as a result of the jump

By contrast here is the identical code with the call left intact and valid

<https://www.virustotal.com/#/file/820eee4d875b32fdc6418fc2da8efae59a12b13e56bdefa1411f90212e262cd8/detection>

3/65 ironically

0x0F0C - February 2, 2018, 11:58 am

(Feb 2, 2018 10:14 AM)ROOTED Wrote: [\[CITE\]](#) Then I opened up in hxd and changed the call to an invalid address

<https://www.virustotal.com/#/file/e57c8d042f467ea92332d42e7819488dbefc272b9338173ad3010a542d063484/detection>

2/65, neither of those detections are as a result of the jump

By contrast here is the identical code with the call left intact and valid

<https://www.virustotal.com/#/file/820eee4d875b32fdc6418fc2da8efae59a12b13e56bdefa1411f90212e262cd8/detection>

3/65 ironically i did a lot of test in this topic
there is no detection because the file is small , if you add APIs and a lot of junk code like that, AVs go nuts

05317832892 - February 2, 2018, 12:15 pm

(Feb 2, 2018 12:58 PM)ivdz Wrote: [\[CITE\]](#) i did a lot of test in this topic
there is no detection because the file is small , if you add APIs and a lot of junk code like that, AVs go nuts

What kind of APIs do you use? Does execution ever reach the junk code in your stub?

0x0F0C - February 2, 2018, 12:31 pm

(Feb 2, 2018 01:15 PM)ROOTED Wrote: [\[CITE\]](#) What kind of APIs do you use? Does execution ever reach the junk code in your stub?

it doesn't matter , any apis will trigger them . And yeah , i tested both situations.

05317832892 - February 2, 2018, 2:19 pm

(Feb 2, 2018 01:31 PM)ivdz Wrote: [\[CITE\]](#) it doesn't matter , any apis will trigger them . And yeah , i tested both situations.

Any variation in the sizes of the data encoded?

Have you tried hiding it in export names?

ganstephanos - February 2, 2018, 3:32 pm

(Jan 30, 2018 06:01 PM)Blanc0 Wrote: [\[CITE\]](#) Private use, targeted machines

no spreading

to bad no programmer doesn't see the honeypot of money opportunity here
Get a private crypt/crypter done/made.