

Forum:[Hack Forums](#)

Thread: [Scammed By EncryptX \\$198 LR](#)

GearCEO™ - February 1, 2013, 8:07 am

Profile ID: <https://hackforums.net/member.php?action=profile&uid=1222379>

Basically, I purchased his encryptx source via LR \$198. I am posting this again because he sold me his shitty source which is TOTALLY PUBLIC.

[My Previous Thread:](#)

As you can see that he didn't give me the source that is why I opened scam report against him but I thought its solved because he gave me the source code that is why I closed this. But he actually gave me public source. Let start what I get from him for \$198 LR.

Stub:

Most of the features do persist but they're all copy pasted. He uses "legit modules" and fake APIs, and fake shit in the resources to confuse most of the anti-viruses.

Just to show how much junk that skid used, here's the size of the stub before I removed all the junk:

[img]<http://img692.imageshack.us/img692/3209/1c28036e85f24234b1af0b5r.png>[/img]

This is after:

[img]<http://img854.imageshack.us/img854/4961/74c4dbb5623440f4b310ed0.png>[/img]

He uses public "dynamic invoke" method using emit to invoke the RunPE with the decrypted server. This method got recently detected and I believe that he decided to sell his crypter source because of that.

There are many similar but he used this exact one.

Stub Before Junk Removal:

http://scan4you.net/result.php?id=69c24_3aet47

After:

http://scan4you.net/result.php?id=7db5a_3aeskm

Kinda pathetic to see that he didn't even encrypt the strings.

Now RunPE:

- It seems like he uses only 2 RunPE's.

The first one: Sikandar's RunPE that was contained in one of his public sources.

The second one: a RunPE that was first seen in xCocaine's Destiny Crypter.

<http://ideone.com/8xq8y>

Next, I proceeded to the crypter itself that was basically flooded with simple checks and anti-debug protections which took me like 10 minutes to remove them all completely.

After I've fixed the source I went to check the storage method.

The storage method that this crypter uses is very old and I think that he changed it before he sold me the source as the crypter won't even crypt things properly.

So the product / source I received is public, corrupted and has nothing in it that worth even 1 single dollar.

The RunPE is public, the invoke method is public, the storage method is public, the scanner has been copy pasted from Banksy's public scan4you scanner source and I completely wasted your money.

Full list of features that don't work

- Extensions Spoofer
- 4 RunPEs (out of 5)
- Melt File
- Disable TaskManager
- Disable System Restore
- Disable CMD
- File Persistence
- Process Persistence
- Assembly Information Cloner (semi-usage of cloned file)
- Generate fake assembly information
- Multi-Binder
- All 6 Antis (except Anti-Sandboxie)
- All 3 spreaders
- Block anti-virus websites
- Scanner
- Encryption Password (the crypter uses compiled stub, the random pool crap is just for beauty)
- The stub is corrupted

All the features that do work:

- 1 RunPE
- Start-Up Persistence
- Start-Up
- Anti-Sandboxie
- File Pumper

Only 5 out of 25 features do work which means that 80% of the crypter is fake.

MY LAST WORDS: RETURN MY \$198 LR MAN ????

?4??? - February 2, 2013, 1:32 am

legit scam report hope you will get your money back

DeMoNi - February 2, 2013, 3:10 am

Just to let you know :

I got access to the source code, i Will defend him in two points :

- his dynamic call is private, never saw the one he uses anywhere.
- the storage method is unique and not public.

For the rest, I cant speak about it because I never had access to all the code.

Cape - February 2, 2013, 5:28 am

Legit scam report OP , hope you will get your money back!

GearCEO™ - February 2, 2013, 7:20 am

@DeMoNi: You did see it in a crypter source you've had before and that it is a public invoke method

with lite changes. Also you've recieved a non working crypter source so you're not that much pissed off from these copy pasted.

Encrypting - February 7, 2013, 12:08 pm

He hasn't been on in like 2 weeks... I bought his crypter... What a dumb decision. It was \$15 for 1 MONTH, so I expect FUD most of the time, the 1 month has now ended, but it wasn't FUD for 3 weeks now. I got totally ed by the user and want my money back... Sorry for a little gravedigging(5 days).

IMachavelli - February 28, 2013, 8:55 pm

Unlucky man. I hope you would get the \$190 back again but it is highly unlikely that he would return it.

Good scam report. At least this may prevent other people from buying it.

It seems that he scammed someone else before as well.

TehRaccoon (172) - Last updated 01-23-2013, 07:33 AM

Neutral (0): Sells fake stuff and non working stuff (Sold a crypter source with fake options that had zero code): DONT BUY FROM THIS USER

GearCEO™ - March 5, 2013, 4:08 am

Thanks for all supporting. Well after long wait he is online today. I just pm'ed him again to reply here.

V???g??? - March 5, 2013, 4:23 am

Sad to see that some UB3R's purposes are to scam people and abuse their trust in others.

King of Diamonds - March 5, 2013, 4:25 am

GI with this. Seems like a lot more ub3rs are scamming

King of Diamonds - March 5, 2013, 4:26 am

GI with this. Seems like a lot more ub3rs are scamming

Heresys - March 5, 2013, 8:33 pm

Looks legit scam report bro.. you know what your talking about and i hope you get your money back.. I wouldn't trust him with getting another source..

GearCEO™ - March 6, 2013, 10:07 am

Thanks for supporting guyz. I pm'ed him again and he saw it also but won't reply even he didn't reply me back. STRANGE!

Neal Caffrey - March 6, 2013, 11:51 am

This faggot still owes me 20\$.

Might open a report.

MineSQL - March 6, 2013, 2:17 pm

I do support your claims, and do not mean to defend this user, but where is the payment proof that you send \$198 LR to him?

Heresys - March 6, 2013, 8:36 pm

(Mar 6, 2013 11:07 AM)???????†? Wrote: [CITE](#) Thanks for supporting guyz. I pm'ed him again and he saw it also but won't reply even he didn't reply me back. STRANGE!

Yea thanks for Pming me back also. asking you a question.. ?

Royal ! - March 7, 2013, 7:42 am

(Mar 6, 2013 03:17 PM)MineSQL Wrote: [\[CITE\]](#) I do support your claims, and do not mean to defend this user, but where is the payment proof that you send \$198 LR to him?

EncryptX would have Replied here Way before if this would have been a Fake Report.

GearCEO™ - March 11, 2013, 8:05 am

Just let you know I deleted the old scam report when he gave me the source code. I think he solved the issue but I was wrong. He actually gave me the source code which is not equal to single penny.

Lol7575 - March 12, 2013, 2:59 am

This sucks man, hope you get your money back.

?????Thr????? - June 22, 2013, 10:40 am

Lol'd at this entire thread.

Future note: Never purchase a crypter source from any random member like EncryptX, ESPECIALLY if the source is in VB. Reason being is because most skids on here only know VB and they'll C&P the night away.