

Forum:[Hack Forums](#)

Thread: [\[FREE\] Crypting Service for Native files.](#)

EASY_HAX - September 25, 2017, 2:53 pm

Introduction

As hackdforums learnt me alot, helped me alot, now I will try to help some members with the knowledge I earned.

What's it ?

This is a handmade crypting service for NATIVE FILES meaning it does not support .NET files. I don't use any crypter, meaning I have direct access to source code, making it easy to refund. I will be free as long as I desire it.

What will happen to my file ?

Your exe native file will be firstly turned into bytes array, after what those bytes will be encrypted with a simple but powerful encryption algorithm making them impossible to be flagged by AVs in scantime. Then those bytes will be embedded in the stub that will write, decrypt and finally execute your exe in memory using runPE method.

Is this service FUD ?

This service is not FUD since I conserve methods to bypass all AVs for personal uses. However I will make all my possible to maintain the detection rate under 2/35. Actually it is 1/35 for the public stub.

How to proceed to profit of this service ?

To avoid of being spammed by a wave of kids, I add an anti-skids method. Here is a code that, after decrypted, will give you a key. Then, on the top of the PM you will send me, just include this key, otherwise I will ignore your message. Upload your server wherever in rar or zip with "789" as password and disable anti-Vm.

Here is the code you have to decrypt (easy)

```
Code 103 157 156 147 162 141 164 165 154 141 164 151 157 156 163 040 164 150 145 040 153
145 171 040 151 163 040 042 111 040 167 151 154 154 040 163 143 141 156 040 155 171 040
163 164 165 142 040 157 156 154 171 040 157 156 040 116 157 144 151 163 164 162 151 142
165 164 145 040 141 156 144 040 126 151 162 165 163 103 150 145 143 153 115 141 164 145
042
```

I will start to crypt servers when I have time for.

Hope you will like this service, give feedbacks and improvements on the thread would be appreciated. (Excuses for english mistakes I could have done)

Have fun

Easy_hax.

kevy42 - September 26, 2017, 1:02 pm

I think u dubble posted fam, happens to me aswell

AceVoid - September 27, 2017, 8:32 am

Will it bypass RUNTIME WindowDefender, AVAST, AVG?

Your PMs are full...

darkweb1927 - September 27, 2017, 10:13 am

Nice post. But i don't understand correctly. LUL haha

EASY_HAX - September 27, 2017, 10:44 am

(Sep 27, 2017 08:32 AM)AceVoid Wrote: [\[CITE\]](#) Will it bypass RUNTIME WindowDefender, AVAST, AVG?

Your PMs are full...

Cleaned PMs, I tested against Windows Defender and it bypassed it like charm, will try very soon on Avast.

Nekfeu - September 27, 2017, 12:44 pm

Can bypass smartscreen ?

TY

EASY_HAX - September 27, 2017, 1:28 pm

(Sep 27, 2017 12:44 PM)Nekfeu Wrote: [\[CITE\]](#) Can bypass smartscreen ?

TY

I'm on Win7 so don't have smartscreen, but send me your skype in PM we could test it together.

kevy42 - September 28, 2017, 7:03 am

(Sep 27, 2017 12:44 PM)Nekfeu Wrote: [\[CITE\]](#) Can bypass smartscreen ?

TY

just remove the stub ZoneID than rar it up to prevent it from being readed

LastSession - September 28, 2017, 7:07 am

Cool but how do you want to bypass runtime protection? Even if you have AES encryption or whatsoever as soon as the file is executed it will be detected. Just saying

EASY_HAX - September 28, 2017, 9:03 am

(Sep 28, 2017 07:07 AM)LastSession Wrote: [\[CITE\]](#) Cool but how do you want to bypass runtime protection? Even if you have AES encryption or whatsoever as soon as the file is executed it will be detected. Just saying

It's injected into memory with runPE method, meaning nothing is written on hard disk.

LastSession - September 28, 2017, 9:06 am

(Sep 28, 2017 09:03 AM)EASY_HAX Wrote: [\[CITE\]](#) It's injected into memory with runPE method, meaning nothing is written on hard disk.

Thanks for clarifying that. You should still get 2/32 or so without anti-emulation but for a free one it's good enough

EASY_HAX - September 28, 2017, 10:04 am

(Sep 28, 2017 09:06 AM)LastSession Wrote: [\[CITE\]](#) Thanks for clarifying that. You should still get 2/32 or so without anti-emulation but for a free one it's good enough

Yeah it's 2/35 Avira and Eset flag it, but i'm currently working on api hooking to get better results.

kevy42 - September 28, 2017, 12:40 pm

(Sep 28, 2017 10:04 AM)EASY_HAX Wrote: [\[CITE\]](#) Yeah it's 2/35 Avira and Eset flag it, but i'm

currently working on api hooking to get better results.

Im pretty sure avira is a string/custom name based detection, also is it a public RunPE?, modified?

EASY_HAX - September 28, 2017, 12:49 pm

(Sep 28, 2017 12:40 PM)WeedmasterOG Wrote: [\[CITE\]](#) Im pretty sure avira is a string/custom name based detection, also is it a public RunPE?, modified?

Already changed strings a couple of times and avira still flag it, I guess it's due to AV's emulation. Yeah it is a modified runPE class.

keyv42 - September 28, 2017, 1:13 pm

(Sep 28, 2017 12:49 PM)EASY_HAX Wrote: [\[CITE\]](#) Already changed strings a couple of times and avira still flag it, I guess it's due to AV's emulation.

Yeah it is a modified runPE class.

Almost all avira detections iv had were dropper.tr and gen, most removed by changing strings, i rarely do get avira to drop me an Fbomb and detrct an actual peace of code, last time it was The memory check call. I dont get string based detections anymore, my usg scrables all custom names in the stub

marcussloane20 - September 28, 2017, 1:31 pm

I need your assistance please PM me

EASY_HAX - September 28, 2017, 1:54 pm

(Sep 28, 2017 01:13 PM)WeedmasterOG Wrote: [\[CITE\]](#) Almost all avira detections iv had were dropper.tr and gen, most removed by changing strings, i rarely do get avira to drop me an Fbomb and detrct an actual peace of code, last time it was The memory check call. I dont get string based detections anymore, my usg scrables all custom names in the stub

Avira flags "Malware detected"

But I take notes of what you say and will do more tests when I get time to. Thanks

keyv42 - September 28, 2017, 2:03 pm

(Sep 28, 2017 01:54 PM)EASY_HAX Wrote: [\[CITE\]](#) Avira flags "Malware detected"

But I take notes of what you say and will do more tests when I get time to. Thanks
GI

Twistd - September 28, 2017, 11:56 pm

(Sep 28, 2017 10:04 AM)EASY_HAX Wrote: [\[CITE\]](#) Yeah it's 2/35 Avira and Eset flag it, but i'm currently working on api hooking to get better results.

This right here makes no sense to me. Avira is usually due to resources, apis, iat hash or strings. Start with adding a junk string table as resource stolen from another file(resource hacker is great to test this with). Then make sure all apis are encrypted, then add some junk api calls. If none of that works, start commenting code to find out where it comes from.

Keep in mind that you should look at your storage method as well. If you store it as a random name in resources it may be detected. Usually MAKEINTRESOURCE(22) up to 37 is good.

Shuffle your compiler settings may also do wonders.