

Forum:[Hack Forums](#)

Thread: [Preview: Sonya Crypter | Native | USG | Stub Builder |](#)

Codefuser - June 27, 2016, 6:13 pm

Sonya Crypter is a crypter written in Autolt. The focus of Sonya Crypter is having a strong USG algorithm and FUD results. Currently I am using a RunPE written in Autolt (No shellcode or public RunPE) which is Runtime UD (a few AV detect it, I will try some other methods to achieve fully FUD runtime result soon, especially the Map/Unmap method which doesn't remove the original image from memory). Dynamic RunPE will also be added which detects which AV is running and choose the appropriate RunPE to bypass it.

What I am working on:USG (String Encryption is the only thing left)

Persistence

Cloud Based Stub Builder

A GUI

Anti Memory Scanner (almost done, it will be in a shellcode)

USG features:Junk code generator

Junk function generator

String encryption

String masking (Using Chr with math generation algorithm)

Flow Obfuscation (Then main trick, creates 95% different stubs not counting the interpreter)

Customizeable stub

UPX or not UPX

Other features:Persistence (both self and injection, using a combination of Watchdog and a few other private methods)

Attempt to bypass UAC using Wusa method (maybe it won't be implemented, I have only started testing this concept a few days ago)

.NET support

Store data as Resource or EOF data

Sleep

Custom injection

Anti Mem Scan

Dynamic injection, injects into a different process if the one injected into is killed

Binder

Anti emulation

AV Disabler (maybe...)

Current scan: NoDistribute.com/result/image/mSrsLMp51P8U7lu4gQXjKNiEhwBq.png
please someone post this as an image for me.

Private Stub also possible as I am only adding resource/EOF data to the stub when crypting it.
Videos bypassing AVs on runtime will be created soon, I just need to tweak and work with the USG some more.

Hoping to see more suggestions and ideas from you, also for pricing as well.

My skype is hiddenintelligence, add me if you have questions. Don't ask about sales, I got a beta tester already

Screenshots Spoiler ([Click to View](#))
Stub Builder

Armitage - June 27, 2016, 6:19 pm

if you can really code in ASM, why do you use Autolt in such thing ??

Codefuser - June 27, 2016, 6:23 pm

(Jun 27, 2016 06:19 PM)Armitage Wrote: [CITE](#) if you can really code in ASM, why do you use Autolt in such thing ??

First of all, I never said I could code in ASM. I can read some though, only started that language a short while ago

Secondly, I am using Autolt since a very strong USG could be implemented for it. Stub in C++ might be considered at a later date.

MrKebab - June 27, 2016, 6:27 pm

(Jun 27, 2016 06:23 PM)Codefuser Wrote: [CITE](#) First of all, I never said I could code in ASM. I can read some though, only started that language a short while ago

Secondly, I am using Autolt since a very strong USG could be implemented for it. Stub in C++ might be considered at a later date.

Wardow's crypter disappears because he got banned.

Then this "new" person appears with the same stuff

?

FunctionDev - June 27, 2016, 6:29 pm

(Jun 27, 2016 06:27 PM)MrKebab Wrote: [\[CITE\]](#) Wardow's crypter disappears because he got banned.

Then this "new" person appears with the same stuff

?

Good find.

Armitage - June 27, 2016, 6:32 pm

(Jun 27, 2016 06:23 PM)Codefuser Wrote: [\[CITE\]](#) First of all, I never said I could code in ASM. I can read some though, only started that language a short while ago

Secondly, I am using Autolt since a very strong USG could be implemented for it. Stub in C++ might be considered at a later date."Anti Memory Scanner (almost done, it will be in a shellcode)"

you can code shellcode but you can't code in ASM right ?

can you explain me what is a memory scanner ? i always see this shit here.. lol

Fluffy_ - June 27, 2016, 6:33 pm

(Jun 27, 2016 06:27 PM)MrKebab Wrote: [\[CITE\]](#) Wardow's crypter disappears because he got banned.

Then this "new" person appears with the same stuff

?

I don't think it's wardow. For one, he's on vacation or something, and right before he was exiled, he implemented a c-shellcode stub that replaced the autoit one.

However, the native stub got detected rather quickly, so he may have rolled it back. Hm, it might actually be wardow.

EDIT: I just remembered that wardow was showing me a new way of obfuscating strings with "String masking (Using Chr with math generation algorithm)". Yep, it's Wardow.

MrKebab - June 27, 2016, 6:35 pm

(Jun 27, 2016 06:33 PM)Fluffy_ Wrote: [\[CITE\]](#) I don't think it's wardow. For one, he's on vacation or something, and right before he was exiled, he implemented a c-shellcode stub that replaced the autoit one.

However, the native stub got detected rather quickly, so he may have rolled it back. Hm, it might actually be wardow.

Ofcourse its wardow, just look through his posts and compare pattern and crypter progress :) I don't even know him and i spotted this instantly.

Codefuser - June 27, 2016, 6:35 pm

(Jun 27, 2016 06:32 PM)Armitage Wrote: [\[CITE\]](#) "Anti Memory Scanner (almost done, it will be in a shellcode)"

you can code shellcode but you can't code in ASM right ?

can you explain me what is a memory scanner ? i always see this shit here.. lol

Memory scanner scans memory the way the scan files. So without it the moment you put the decrypted stub in memory, it is detected

And who is Wardow? Link me

Armitage - June 27, 2016, 6:38 pm

(Jun 27, 2016 06:35 PM)Codefuser Wrote: [\[CITE\]](#) Memory scanner scans memory the way the scan files. So without it the moment you put the decrypted stub in memory, it is detected

And who is Wardow? Link melol nice story, have a good day.

Fluffy_ - June 27, 2016, 6:39 pm

(Jun 27, 2016 06:35 PM)Codefuser Wrote: [\[CITE\]](#) Memory scanner scans memory the way the scan files. So without it the moment you put the decrypted stub in memory, it is detected

And who is Wardow? Link me

Very funny. I don't believe that you're allowed to have multiple accounts, especially after you were banned.

EDIT: Reported for profile violation.

MrKebab - June 27, 2016, 6:41 pm

(Jun 27, 2016 06:39 PM)Fluffy_ Wrote: [\[CITE\]](#) Very funny. I don't believe that you're allowed to have multiple accounts, especially after you were banned.

(Jun 27, 2016 06:33 PM)Fluffy_ Wrote: [\[CITE\]](#) EDIT: I just remembered that wardow was showing me a new way of obfuscating strings with "String masking (Using Chr with math generation algorithm)". Yep, it's Wardow.

Yuuuuuuup, busted.

+1

Codefuser - June 27, 2016, 6:46 pm

(Jun 27, 2016 06:39 PM)Fluffy_ Wrote: [\[CITE\]](#) Very funny. I don't believe that you're allowed to have multiple accounts, especially after you were banned.

Are you talking about hackforums.net/member.php?action=profile&uid=1810243 ?

I have just looked at his anti emulator and it is different than mine (even though it looks fairly interesting, might try that once I have finished ASM). Mine uses heavy calculation and stuffs like that to have a realistic delay.

Edit: and based on his thread, he is using C and not autoit?

Fluffy_ - June 27, 2016, 6:48 pm

(Jun 27, 2016 06:46 PM)Codefuser Wrote: [\[CITE\]](#) Are you talking about hackforums.net/member.php?action=profile&uid=1810243 ?

I have just looked at his anti emulator and it is different than mine (even though it looks fairly interesting, might try that once I have finished ASM). Mine uses heavy calculation and stuffs like that to have a realistic delay.

Edit: and based on his thread, he is using C and not autoit?

Come on man, you were telling me about trying to figure out how to do an anti-emulator in asm by calculating primes or something like that. We all know that you're wardow.

And he switched to autoit to c, but you would know that.

Codefuser - June 27, 2016, 6:51 pm

(Jun 27, 2016 06:48 PM)Fluffy_ Wrote: [\[CITE\]](#) Come on man, you were telling me about trying to figure out how to do an anti-emulator in asm by calculating primes or something like that. We all know that you're wardow.

And he switched to autoit to c, but you would know that.

I am doing that in AutoIt?

Code \$i = 0

\$nums = NULL

\$to = Random(10000, 90000, 1)

Do

```
$f = ChrW(34)
```

```
$i += 1
```

```
If _isprime($i) Then[/php]
```

```
    $nums &= "j" & $i
```

```
EndIf
```

Until \$i = \$to

```
$exp = StringSplit($nums, "j")
```

```
$f_num = $exp[Random(15, 25, 1)] & Random(1500, 2500, 1)
```

```
$f_num_2 = $exp[Random(1, 14, 1)] & Random(1500, 2500, 1)
```

```
$f_num_4 = Random(1500, 2500, 1)
```

```
$sin = $f_num_4^2
```

```
$f_num_5 = $sin^3
```

Please, stop attacking me. I joined this forums hoping to sell my product here and a few minutes after some people started saying that I violate forums rule. I assure you I have read the Help Doc and have not violated a rule here during the few hours that I were here. Please someone tell staff to check my IP against Wardow.

and also if I am correct, Profile Violation only covers putting offensive/religious/political sutffs in your profile, not muti accounting.

And based on what Wardow said, his anti emulator allocates memory to break them only, not doing calculations and maths.

MrKebab - June 27, 2016, 6:51 pm

(Jun 27, 2016 06:46 PM)Codefuser Wrote: [\[CITE\]](#) Are you talking about hackforums.net/member.php?action=profile&uid=1810243 ?

I have just looked at his anti emulator and it is different than mine (even though it looks fairly interesting, might try that once I have finished ASM). Mine uses heavy calculation and stuffs like that to have a realistic delay.

Edit: and based on his thread, he is using C and not autoit?

I enjoy watching you trying to defend yourself but the defense is already blown to bits in this thread.

Codefuser - June 27, 2016, 6:56 pm

(Jun 27, 2016 06:51 PM)MrKebab Wrote: [\[CITE\]](#) I enjoy watching you trying to defend yourself but the defence is already blown to bits in this thread.

Please, give me solid proof, not just some "educated guesses" (that are actually very uneducated).

Just get off my thread and leave me in peace. Please.

MrKebab - June 27, 2016, 6:58 pm

(Jun 27, 2016 06:56 PM)Codefuser Wrote: [\[CITE\]](#) Please, give me solid proof, not just some "educated guesses" (that are actually very uneducated).

Just get off my thread and leave me in peace. Please.

Admin will check the patterns.. It's quite easy to spot.

Just because you grabbed a new ip from vip72 doesnt mean you're a new person :)

Fluffy_ - June 27, 2016, 6:59 pm

(Jun 27, 2016 06:51 PM)Codefuser Wrote: [\[CITE\]](#) I am doing that in AutoIt?

```

Code    $i = 0
$num = NULL
$to = Random(10000, 90000, 1)
Do
    $f = ChrW(34)
    $i += 1
    If _isprime($i) Then[/php]
        $num &= "j" & $i
    EndIf

Until $i = $to
$exp = StringSplit($num, "j")
$f_num = $exp[Random(15, 25, 1)] & Random(1500, 2500, 1)

$f_num_2 = $exp[Random(1, 14, 1)] & Random(1500, 2500, 1)
$f_num_4 = Random(1500, 2500, 1)
$sin = $f_num_4^2
$f_num_5 = $sin^3

```

Please, stop attacking me. I joined this forums hoping to sell my product here and a few minutes after some people started saying that I violate forums rule. I assure you I have read the Help Doc and have not violated a rule here during the few hours that I were here. Please someone tell staff to check my IP against Wardow.
and also if I am correct, Profile Violation only covers putting offensive/religious/political sutffs in your profile, not muti accounting.

And based on what Wardow said, his anti emulator allocates memory to break them only, not doing calculations and maths.
That was in a post from a while back that you would have to spend a lot of time looking at his profile to find. (I stand corrected on this one)
Look man, I know that i got peeved at you before, but there was simply no reason to go up and block me on everything. gg.

Also, "2. We do not allow multiple accounts except a UID_TEMP account as explained in our "Stolen and Lost HF Accounts" help doc."

???? - June 27, 2016, 7:00 pm
Joined: Today

You are a multi counter.

Codefuser - June 27, 2016, 7:00 pm
(Jun 27, 2016 06:59 PM)Fluffy_ Wrote: [\[CITE\]](#) That was in a post from a while back that you would have to spend a lot of time looking at his profile to find.
Look man, I know that i got peeved at you before, but there was simply no reason to go up and block me on everything. gg.

Also, "2. We do not allow multiple accounts except a UID_TEMP account as explained in our "Stolen and Lost HF Accounts" help doc."
dude, that post was like on the first page of his threads when I used the FInd Users THread button.
Update: Second result. SECOND RESULT.

???? - June 27, 2016, 7:04 pm

(Jun 27, 2016 07:00 PM)Codefuser Wrote: [\[CITE\]](#) dude, that post was like on the first page of his threads when I used the Find Users Thread button. Update: Second result. SECOND RESULT. What country are you from Mr. Codefuser?

Codefuser - June 27, 2016, 7:07 pm

(Jun 27, 2016 07:04 PM)ScorpiOn Wrote: [\[CITE\]](#) What country are you from Mr. Codefuser? America, why?

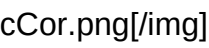
gyazo.com/acccfe8016788bdf92fc9910f4a7e800

oO_Matrix_Oo - June 27, 2016, 10:28 pm

leave him alone, this guy is not wardow since he is right there smh

SIM-1676753 - June 27, 2016, 10:30 pm

oO_Matrix_Oo - June 27, 2016, 10:32 pm

(Jun 27, 2016 10:30 PM)Virility Wrote: [\[CITE\]](#) [img] yes cunfirmed.

Oliver Sykes - June 27, 2016, 10:38 pm

You guys are silly. Wardrobe has shitty English compared to this guy...or anyone else.

oO_Matrix_Oo - June 27, 2016, 10:40 pm

(Jun 27, 2016 10:38 PM)Oliver Sykes Wrote: [\[CITE\]](#) You guys are silly. Wardrobe has shitty English compared to this guy...or anyone else. It's not even true, you lie.

???? - June 27, 2016, 10:40 pm

(Jun 27, 2016 10:38 PM)Oliver Sykes Wrote: [\[CITE\]](#) You guys are silly. Wardrobe has shitty English compared to this guy...or anyone else. Ok then this is another member who has been banned here. Probably MagicMushroom.

EDIT: LOOOLLL he upgraded first day tf is that

oO_Matrix_Oo - June 27, 2016, 10:44 pm

(Jun 27, 2016 10:40 PM)ScorpiOn Wrote: [\[CITE\]](#) Ok then this is another member who has been banned here. Probably MagicMushroom. MagicMushroom is BlackCat that was also banned I think he got banned after I reported that to Omniscient

???? - June 27, 2016, 10:44 pm

(Jun 27, 2016 10:44 PM)oO_Matrix_Oo Wrote: [\[CITE\]](#) MagicMushroom is BlackCat that was also banned I think he got banned after I reported that to Omniscient Yeah this is his 3rd multi I think lol.

oO_Matrix_Oo - June 27, 2016, 10:46 pm

(Jun 27, 2016 10:44 PM)ScorpiOn Wrote: [\[CITE\]](#) Yeah this is his 3rd multi I think lol. At one point I think you just need to stop trying to sell things and create accounts just to visit and lurk around

Mace - June 27, 2016, 11:23 pm

Stop making a conclusion already. If this happens to be wardow, he should obviously be banned, but if not, he shouldn't be attacked by other posters this way. Report him to omniscient, and he will make a conclusion, as he's the only one who can.

Codefuser - June 28, 2016, 6:51 am

(Jun 27, 2016 10:40 PM)ScorpiOn Wrote: [\[CITE\]](#) Ok then this is another member who has been banned here. Probably MagicMushroom.

EDIT: LOOOLLL he upgraded first day tf is that becuz I want gauth?

Please, staff, check my IP agaisnt all the past IPs of Wardow. I am not using a proxy, using a clean connection here.

Edit: Just talked to BlackCat (found his skype).

you can join this skype group: <https://join.skype.com/o7jMQc04C1fi> and me and black cat will demonstrate our accents to you.

MrKebab - June 28, 2016, 2:37 pm

(Jun 28, 2016 06:51 AM)Codefuser Wrote: [\[CITE\]](#) becuz I want gauth?

Please, staff, check my IP agaisnt all the past IPs of Wardow. I am not using a proxy, using a clean connection here.

Edit: Just talked to BlackCat (found his skype).

you can join this skype group: and me and black cat will demonstrate our accents to you.

Your whole way of reacting to these accusations is just wrong..

You go totally in defense mode... A normal sane person would not react like this, quite funny.

So you wanted l33t for gauth, funny.. If you wanted it so bad, wouldnt you already activated it?

Gauth/2FA: Not Activated

Codefuser - June 28, 2016, 3:32 pm

(Jun 28, 2016 02:37 PM)MrKebab Wrote: [\[CITE\]](#) Your whole way of reacting to these accusations is just wrong..

You go totally in defense mode... A normal sane person would not react like this, quite funny.

So you wanted l33t for gauth, funny.. If you wanted it so bad, wouldnt you already activated it?

Gauth/2FA: Not Activated

because I was busy and I actually have a life?

Dr. Plague - June 28, 2016, 5:20 pm

Add some screenshot's! Anyway, look's good! I hope to see release soon.:)

Codefuser - June 28, 2016, 5:48 pm

(Jun 28, 2016 05:20 PM)Dr.Plague Wrote: [\[CITE\]](#) Add some screenshot's! Anyway, look's good! I hope to see release soon.:)

Creating the GUI for the stub builder.

atomic101002 - June 28, 2016, 11:10 pm

Thx bro i rly needeed this

iLogic™ - June 28, 2016, 11:51 pm

Yet another copy & pasta... Anyways good luck.

Codefuser - June 29, 2016, 5:41 am

(Jun 28, 2016 11:51 PM)iLogic™ Wrote: [\[CITE\]](#) Yet another copy & pasta... Anyways good luck.
LOL I typed it completely from scratch.

aesad - June 29, 2016, 12:45 pm

Good luck Codefuser with that. Looks like good crypter.

Goldmouth - June 29, 2016, 6:41 pm

AV Disabler. Cant wait to test this out.

Codefuser - June 29, 2016, 7:18 pm

(Jun 29, 2016 06:41 PM)Hostah Wrote: [\[CITE\]](#) AV Disabler. Cant wait to test this out.
You already did with the basic feature xD
AV disabler will take a while, anyway thanks for paying just to test it.

Updated OP with screenshot of stub builder. The blank area is for a logo (which will come soon)

Hopsin - June 30, 2016, 2:25 pm

I like the simplicity of the GUI. Good luck buddy if you decide to release/sell it or whatever you do.
Have a nice day !

Codefuser - July 1, 2016, 11:03 am

New GUI with a fresh Logo. Thanks to Fluffy_ for designing it

Dr. Plague - July 1, 2016, 11:05 am

(Jul 1, 2016 11:03 AM)Codefuser Wrote: [\[CITE\]](#) New GUI with a fresh Logo. Thanks to Fluffy_ for designing it

Look's good! ?

Codefuser - July 2, 2016, 3:35 pm

Updated thread with a poll. The free version will also have limited features, of course

Codefuser - July 6, 2016, 10:56 pm

Adding a junk resource tool that generates long random English strings that are thrown together and slapped into the executable.

DeluxeSoftware - July 7, 2016, 1:12 pm

@all
This guy is not Wardow or Blackcat.
Wardow kinda hates me and his English is not as good as Codefuser's. Blackcat's English is even worse. He can't even write correct German sentences.

Codefuser - July 7, 2016, 2:05 pm

(Jul 7, 2016 01:12 PM)DeluxeSoftware Wrote: [\[CITE\]](#) @all
This guy is not Wardow or Blackcat.
Wardow kinda hates me and his English is not as good as Codefuser's. Blackcat's English is even worse. He can't even write correct German sentences.

Thank you. Hope that cleared some doubts

Edit: Adding an injection method for PIC such as FormBook, DarkHotel, etc that will be 100% runtime FUD since it is very simple and generic compared to normal RunPE.

DataByte - July 7, 2016, 3:52 pm

Will you be releasing this crypter as paid?

Codefuser - July 7, 2016, 5:43 pm

(Jul 7, 2016 03:52 PM)DataByte Wrote: [\[CITE\]](#) Will you be releasing this crypter as paid? Yes?

There will be a lite edition which will be free and available for a short time as well.

DataByte - July 7, 2016, 6:06 pm

(Jul 7, 2016 05:43 PM)Codefuser Wrote: [\[CITE\]](#) Yes?

There will be a lite edition which will be free and available for a short time as well.

That's cool man! Best of luck with sale's! (When released)?

Demoralise - July 9, 2016, 1:40 am

(Jul 7, 2016 01:12 PM)DeluxeSoftware Wrote: [\[CITE\]](#) @all

This guy is not Wardow or Blackcat.

Wardow kinda hates me and his English is not as good as Codefuser's. Blackcat's English is even worse. He can't even write correct German sentences. Well coming from somebody who actually is friends with Wardow I must say that Codefuser's English level and the way they write their sentences is very similar to the way Wardow would.

Is it Wardow? Nobody knows.

Codefuser - July 10, 2016, 2:03 pm

Working on patching module path right now, struggling a bit with it but hoping to finish it in the next 2 weeks.