

Forum:[Hack Forums](#)

Thread: [encrypted exe video](#)

amaluno.m - June 14, 2016, 6:48 am

Hi everyone,

I have lots of video tutorials that are encoded with Vaysoft program in the exe format. each time I want to play the video on a new machine, I have to obtain a registration code for the new machineID , it is frustrating!

when the exe video is playing, an avi file is created in the windows temp folder, but that avi seems to be encrypted too and can not be played.

can you please help me to extract the videos file from these annoying exe's?!

here is one of the exe video files:

mega.nz/#!A0ZATlaZ!uuODBKf7DnXlbWnizvToAyoDXZCbUSycbX-iLL_Pf5M

BlackHat0009 - June 17, 2016, 12:58 pm

Yes i can help email me BlackHat0009atgmail.com you'r old password also for this video.exe

The OG FurFag ? - June 17, 2016, 1:01 pm

Waiting for people to come crying their infected or some shit.

amaluno.m - June 18, 2016, 1:25 am

(Jun 17, 2016 12:58 PM)BlackHat0009 Wrote: [\[CITE\]](#) Yes i can help email me BlackHat0009atgmail.com you'r old password also for this video.exe

I can give the machineID and registration key.. but please remind that this ID and regkey is unique to every machine. so I beleive that my ID and regkey will not work on your computer.. is there any other way to work around this?

(Jun 17, 2016 01:01 PM)SpamTecCrew Wrote: [\[CITE\]](#) Waiting for people to come crying their infected or some shit.

why so?! I did not post anything harmful! this is just an encrypted video file done in Vaysoft software that I uploaded.

amaluno.m - June 20, 2016, 4:09 am

any body could help to decode this video please ?

BlackHat0009 - June 21, 2016, 10:20 am

i said send password, look everything depends on your response,"try to make this quick don't waste time at least my time"

amaluno.m - June 21, 2016, 2:05 pm

(Jun 21, 2016 10:20 AM)BlackHat0009 Wrote: [\[CITE\]](#) i said send password, look everything depends on your response,"try to make this quick don't waste time at least my time"

ok, here is the password, and thank you for the help:

MachineID: 313050801572982345

Regkey: 8560fe2088f92319ac61c0775c840c02

potatofarmer - June 22, 2016, 7:04 am

Well an alternative to extracting the videos is to just fish some serials, or write a keygen. The exe generates a hwid and then uses that in generating a serial. Then it compares your input serial against the one it generated. So its pretty easy to fish them. Writing a keygen would also be possible since it has all the code you need to rip/rewrite just sitting there. Nothing really needs to much thought just time.

To fish serials, just follow the messagebox retun to the serial check code, or use dede to easily find the function called from the OK button click. Then you follow the that code to the function that does the generation and verification. The string compare is in there. This may seem vague but if you follow any ollydbg serial fishing tutorials it'll probably make more sense.

I did have one problem playing the video though, I didn't see any video and just had audio so I'm guessing I'm missing a codec of some sort? To verify that I'll look in to extracting the video itself from the app like you asked. I'll let you know if thats easier than writing a keygen once I'm done looking through it.

amaluno.m - June 22, 2016, 7:53 am

(Jun 22, 2016 07:04 AM)potatofarmer Wrote: [\[CITE\]](#) Well an alternative to extracting the videos is to just fish some serials, or write a keygen. The exe generates a hwid and then uses that in generating a serial. Then it compares your input serial against the one it generated. So its pretty easy to fish them. Writing a keygen would also be possible since it has all the code you need to rip/rewrite just sitting there. Nothing really needs to much thought just time.

To fish serials, just follow the messagebox retun to the serial check code, or use dede to easily find the function called from the OK button click. Then you follow the that code to the function that does the generation and verification. The string compare is in there. This may seem vague but if you follow any ollydbg serial fishing tutorials it'll probably make more sense.

I did have one problem playing the video though, I didn't see any video and just had audio so I'm guessing I'm missing a codec of some sort? To verify that I'll look in to extracting the video itself from the app like you asked. I'll let you know if thats easier than writing a keygen once I'm done looking through it.

Thank you potatofarmer. Yes you need mediaplayer classic lite codec pack to play the video (which is free for download). I have the password for all these video files but as I mentioned, the problem is I have to play these videos on many other computers and I have to enter a unique code for each of them, which is absolutely unpractical and annoying!

I don't know why they did so, because I had paid for these video tutorials! and I just want the videos :)

potatofarmer - June 22, 2016, 8:38 am

Well installing k-lite codec pack fixed the video problem on my VM. So it looks like serial fishing really is a pretty easy solution. I'm gonna reread the rules here and see how much info I can post without violating them.

Alright, read the rules and it looks like providing serial fishing directions, a keygen, or even serials would be a solid violation of them. So the bad news is that I can't provide you with the detailed info on how to get serials without violating those rules.

As for the video data, I took a quick look and only saw it write out a giant empty video file, so i'm guessing everything is in memory somewhere. So the best I can recommend is that you take a little time to read up on ollydbg, and follow some serial fishing tutorials. This app is susceptible to serial fishing and its not protected by anything serious. After you do it once or twice, you'll be able to get a

serial for it in a couple minutes with ollydbg on your new machine.

amaluno.m - June 22, 2016, 1:04 pm

(Jun 22, 2016 08:38 AM)potatofarmer Wrote: [\[CITE\]](#) Well installing k-lite codec pack fixed the video problem on my VM. So it looks like serial fishing really is a pretty easy solution. I'm gonna reread the rules here and see how much info I can post without violating them.

Alright, read the rules and it looks like providing serial fishing directions, a keygen, or even serials would be a solid violation of them. So the bad news is that I can't provide you with the detailed info on how to get serials without violating those rules.

As for the video data, I took a quick look and only saw it write out a giant empty video file, so i'm guessing everything is in memory somewhere. So the best I can recommend is that you take a little time to read up on ollydbg, and follow some serial fishing tutorials. This app is susceptible to serial fishing and its not protected by anything serious. After you do it once or twice, you'll be able to get a serial for it in a couple minutes with ollydbg on your new machine.

potatofarmer, thank you for your time. may I have your email? mine is: amaluno.m at gmail .com when the video plays, it stops every 4:25 minutes. I guess they have set this timer to prevent screen recording! do you also have a solution to play the videos without being halted every 4:25 minutes?

fijasko - June 22, 2016, 4:30 pm

```
0049A4BA    mov     eax,dword ptr [ebp-0C] ; correct serial
0049A4BD    mov     edx,dword ptr [ebp-4]  ;your serial
0049A4C0    call    @LStrCmp
0049A4C5>   jne     0049A4C9 ; je good boy/jne bad boy
```

Breakpoint on 0049A4C0 .EAX will hold the correct serial :)
Reenter it and that's all. Or you can just nop the jne or chage it to je.

(You will find it in here HKEY_CURRENT_USER\Software\waysoft\videotoexe\ in case you need it)

amaluno.m - June 23, 2016, 6:29 am

(Jun 22, 2016 04:30 PM)fijasko Wrote: [\[CITE\]](#) 0049A4BA mov eax,dword ptr [ebp-0C] ;
correct serial
0049A4BD mov edx,dword ptr [ebp-4] ;your serial
0049A4C0 call @LStrCmp
0049A4C5> jne 0049A4C9 ; je good boy/jne bad boy

Breakpoint on 0049A4C0 .EAX will hold the correct serial :)
Reenter it and that's all. Or you can just nop the jne or chage it to je.

(You will find it in here HKEY_CURRENT_USER\Software\waysoft\videotoexe\ in case you need it)
fijasko,

Thank you. It WORKED !!! as you see I have found the 0049A4C5 and other addresses you mentioned. I changed the JNZ to JE in 0049A4C5 and then I exported the file. Now each time when it still asks for serials, I just enter 123 or whatever and it plays the video. Awesome! I am not allowed to post images here until I post 50 posts, but here is the screenshot: i.imgsafe.org/bfde46d5ce.jpg

Unfortunately my knowledge of assembly and debugging is nearly zero! and I have lots of these videos. Do I have to do this on each of them?

And also, they have set some timer in the video playback, so it stops at time 4:25 of the video (and again at 4:25+4.25= 8:50) and so on! I assume they did it to prevent screen recording.. is there any way to also disable this timer?!

and again, thank you fijasko for the help so far :)

BlackHat0009 - June 23, 2016, 11:08 am

Look's like i'm late but never mind.

i have another alternative basically this is a #Pa#tch# so it goes like this:

```
0049A4BA mov eax,dword ptr [ebp-0C] ; correct serial
0049A4BD mov edx,dword ptr [ebp-4] ;your serial
0049A4C0 call @LStrCmp
0049A4C5> jne 0049A4C9 ; je good boy/jne bad boy
```

change only this line to

```
0049A4BA mov eax,dword ptr [ebp-0C] ; correct serial
0049A4BD mov edx,dword ptr [ebp-4] ;your serial
0049A4C0 call @LStrCmp
0049A4C5> jmp 0049A4C9 ; je good boy/jne bad boy
```

Enter you'r old password and it will work fine. And Yes this program.exe uses some system process enumeration function or Win32 API so that while .exe is running no one can run screen recording software program. and again video's .mp4 are running in memory. Basically premium version of this software first creating a temporary virtual Drive in your system and then second decrypting .mp4 into this drive. and playing video from there.

Enjoy!!

amaluno.m - June 23, 2016, 11:36 am

Thank you blackhat0009, I learned some thing new from you and fijasko :)

actually I can easily record the screen while the video is playing, but the stops at 4:24 and I have to play it again from 4:26. The screen recorder runs OK all the time. I wish there was a work around to prevent it from stopping at 4:24

BlackHat0009 - June 24, 2016, 1:10 pm

Hello amaluno.m

by the way, there was a typing mistake actually it look like this:

```
0049A4BA  8B45 F4      MOV     EAX, DWORD PTR SS:[EBP-C]      ; ntdll.7797E115
0049A4BD  8B55 FC      MOV     EDX, DWORD PTR SS:[EBP-4]
0049A4C0  E8 43A1F6FF  CALL    <4.System.@LStrCmp>
0049A4C5  90           NOP                                     ; jump taken <----- change this to
NOP
0049A4C6  90           NOP
0049A4C7  B3 01       MOV     BL, 1
```

Enjoy lifetime video with your old password.

Q.Why you want to record screen ?

I don't think you have to do that because this video will now run for lifetime on any system.

Yes, there is always a patch for any function inside any program but why do that ? because now you have so called "master key" for any system.

Thank You ALL!!

amaluno.m - June 25, 2016, 2:40 am

Blackhat0009, thank you for the update.

Yes, I have a lifetime playback, so I will not screen record the video. The problem is it stops at 4:25 and this is really annoying. because I have to play it again and search for the place where it left off. Don't you have this problem when you play the video? doesn't it crash on 4:24?

BlackHat0009 - June 25, 2016, 10:21 am

No problemmmoooo Dear

I have no problem video is running just fine.

I have enter password as random integer and video.exe is running till end. Not even blink.

For me 100% working no problem.

I think you have virus in your system try to install/update antivirus else format windows.

Please remove mega.nz/#!A0ZATlaZ!uuODBKf7DnXlbWnizvToAyoDXZCbUSycbX-iLL_Pf5M

Download Link before someone gets into trouble.

Thank you

And i'm out of here.

amaluno.m - June 25, 2016, 12:03 pm

Thank you blackhat, thank you all guys ! problem solved, mission complete ?