

Forum:[Hack Forums](#)

Thread: [Crack or Decompile Request of Windows Program](#)

SIM-2030811 - November 12, 2020, 1:43 am

Hi,

This is a program which streams online courses, and I have pay for that, but they delete the videos after 10 days, and I need to keep them. By the way, I can use a screen recording program to save them, but it takes so long and also as an IT expert, I just went crazy when I can't bypass a security wall. ?

- I have tried to sniff the network using Wireshark, but the connection seems to be encrypted.
- I have tried to decompile the codes so I can find the source or the stream URL, but I am not familiar with this language...

The program developed using: <https://github.com/nwjs/nw.js>

After you install the program, there is the main file which is a .exe file, but you can unzip it using Winrar or any similar program (you can see the screenshot below and also you can download it)

Main Setup File:

https://mega.nz/file/ac4C2D6B#xLORL3fyN7fnZZbabDucwVseAu_ZcmKjpUVKGsr3Hlg

- You should download and install it, its a 32bit program so installed itself to *Program Files (x86)
- There is a main .EXE file in the installed folder which will open a screen (I think its a chromium container) and ask for user and pass.
- I can't share username and pass, but if needed, I can share my PC for it.

* Unzipped .EXE file:

https://mega.nz/file/ORokgliZ#2X8XBanWP_VxJg1-DtRuGaAOJSF08u3jZVmtJ_70r2w

- I was not able to decompile the index.bin file, which I believe contains the connection URL, but I am not sure if we can start to download by finding that URL.

I have not any desire to download and share the videos; I want to keep them for myself as I paid for them.

I can also pay up to 100\$ to someone who can help me download the videos.

Exalted - November 12, 2020, 2:00 am

The application is a web wrapper of <https://portal.tusem.net/>.

If you log in through there, open the Network tab in Dev-Tools and click on a video you can probably get an idea of what is happening.

SIM-2030811 - November 12, 2020, 8:03 am

(Nov 12, 2020 03:00 AM)Exalted Wrote: [\[CITE\]](#) The application is a web wrapper of <https://portal..net/>.

If you log in through there, open the Network tab in Dev-Tools and click on a video you can probably get an idea of what is happening.

nope, if you open it in the browser it just calls different page which wants you to download the program.

Exalted - November 13, 2020, 4:23 am

(Nov 12, 2020 09:03 AM)SIM-2030811 Wrote: [\[CITE\]](#) nope, if you open it in the browser it just calls different page which wants you to download the program.

It's just a wrapper. The website detects whether you're using your browser or using the desktop client and redirects you accordingly. I would need the credentials or access to a computer that is signed in.

VizOne - November 19, 2020, 12:55 am

use fiddler to find credentials and request sending from your pc

SIM-2030811 - November 19, 2020, 1:36 am

I used Fiddler and find some information. Also, I have found the video URL, but the video encrypted with an SSL, which if I activate the Capture HTTPS traffic the video never starts, because of copied SSL.

Actually, there is no need to decrypt the video, if I can mimic what this app does in a browser, I will be able to download the decrypted video.

I can grant access to my PC if you want to test it out.

(Nov 13, 2020 05:23 AM)Exalted Wrote: [\[CITE\]](#) It's just a wrapper. The website detects whether you're using your browser or using the desktop client and redirects you accordingly. I would need the credentials or access to a computer that is signed in.

Yes, it exactly as you just said. But I am not sure how to mimic the program in the browser...

Any idea? I can get access to my PC if you want.

QueensC - November 19, 2020, 1:50 am

perform man in the middle attack, or get the decryption key .

SIM-2030811 - November 19, 2020, 2:55 am

(Nov 19, 2020 02:50 AM)QueensC Wrote: [\[CITE\]](#) perform man in the middle attack, or get the decryption key .

Fiddler is actually a MITM attack, and I can start the video if using the "stream" option in Fiddler. But I can't figure out how to capture the video! Fiddler downloads the video (I can see from the network and also the encrypted codes in raw files of Fiddler) but if the video encrypted then I will not able to use it (I am not sure if it's possible to decrypt it or not!)

But If we can use a browser to log in just like the program (which is chrome in itself) then we can download the decrypted video inside the bowser...

Any idea?

SIM-2030811 - November 21, 2020, 2:57 am

Any idea?

How can I make the chrome act just like this program?

There is a code in login page which redirects the user to different pages. If its a browser then redirect to the download page. But if its the program which open the page, then redirect to video pages.

The program sends a special signal to the server to be able to redirect to the video pages.

andmuchmore - November 21, 2020, 3:16 am

(Nov 19, 2020 03:55 AM)SIM-2030811 Wrote: [\[CITE\]](#) Fiddler is actually a MITM attack, and I can start the video if using the "stream" option in Fiddler. But I can't figure out how to capture the video! Fiddler downloads the video (I can see from the network and also the encrypted codes in raw files of Fiddler) but if the video encrypted then I will not able to use it (I am not sure if it's possible to decrypt it or not!)

But If we can use a browser to log in just like the program (which is chrome in itself) then we can download the decrypted video inside the browser...

Any idea?

I had a quick look at it, the website users the same api endpoint as client but the post data on the website is missing the client_info object.

If you add those values to the website it should allow you to play the videos online.

I don't have a login so I can't help much further.

SIM-2030811 - November 22, 2020, 1:43 am

(Nov 21, 2020 04:16 AM)andmuchmore Wrote: [\[CITE\]](#) I had a quick look at it, the website users the same API endpoint as a client but the post data on the website is missing the client_info object.

If you add those values to the website it should allow you to play the videos online.

I don't have a log in so I can't help much further.

You are right, I saw the same but my knowledge is limited here and I don't know how to find what is missing and how to add the missing part to the browser.

If you have time I can send you SS from Fiddler or any other program you use. Also, I can invite you to my PC (it's safer to login from my IP).