

Forum:[Hack Forums](#)

Thread: [Decompiled VB6 code - need help with finding what it calculates](#)

Kufe - October 30, 2018, 1:40 am

I hope someone can help me with this problem, because I am struggling for 4 days (and a few nights) with this one... I decompiled some small VB6 app which checks for license online. It goes to specific url (.php?id=XXXXXX - where XXXX is some generated HW ID) and returns string with 3 parameters (divided with |). I can use host file to change DNS and use my own returned parameters, but I have a problem with 3rd parameter, because I don't know what it should be. The first parameter has to be OK, second is any name (it's just used to display Welcome NAME), third is the one causing me problems - it's some number I think (usually 3 digit). So returned text is something like OK|Mike|701.

*Solved, thank you AbakBarama.

John Doe 5726 - October 30, 2018, 1:51 am

Would be easier if you sent full binary, your decompiled code makes little sense, also, you should just NOP out the license check instead of bothering to replicate a server response.

Kufe - October 30, 2018, 2:14 am

I don't know how at VB6. It's easy with C# or .NET but here I was only able to decompile with VB decompiler (can modify code and rebuild exe). Full exe is available here - [mega.nz/#!KrgkxYla!4lpvua_31eV_CsTnqzz4uixRej-6KThmb_9zmTVrKwE](#)

John Doe 5726 - October 30, 2018, 2:19 am

(Oct 30, 2018 02:14 AM)Kufe Wrote: [\[CITE\]](#) I don't know how at VB6. It's easy with C# or .NET but here I was only able to decompile with VB decompiler (can modify code and rebuild exe). Full exe is available here - [mega.nz/#!KrgkxYla!4lpvua_31eV_CsTnqzz4uixRej-6KThmb_9zmTVrKwE](#)
Do you have an example of a valid server response with the corresponding HWID?

Can you send it?

Kufe - October 30, 2018, 2:31 am

(Oct 30, 2018 02:19 AM)John Doe 5726 Wrote: [\[CITE\]](#) Do you have an example of a valid server response with the corresponding HWID?

Can you send it? If you send 9A979599C66D9D9D996E9F9A20203356300 returned value is OK|User|703

I think there is something done with second part of that number (20203356300), because first part even if I change in my register it still works.

John Doe 5726 - October 30, 2018, 3:18 am

(Oct 30, 2018 02:31 AM)Kufe Wrote: [\[CITE\]](#) If you send 9A979599C66D9D9D996E9F9A20203356300 returned value is OK|User|703

I think there is something done with second part of that number (20203356300), because first part even if I change in my register it still works.

When you try with your hijacked server response and another PC, the number 703 does not work,

right?

Kufe - October 30, 2018, 3:35 am

It does work.

Also 65976A69686C686365686C6639573726000 correct returned number is 1149.

Also same number for 686C6070626D689B966B9B9439573726000, so I guess the only important part of number where 1149 is generated is 39573726000.

John Doe 5726 - October 30, 2018, 3:41 am

(Oct 30, 2018 03:35 AM)Kufe Wrote: [\[CITE\]](#) It does work.

Also 65976A69686C686365686C6639573726000 correct returned number is 1149.

Also same number for 686C6070626D689B966B9B9439573726000, so I guess the only important part of number where 1149 is generated is 39573726000.

So what is the problem if it does work?

What could that value be?

Does the program have an expiration date? Several plans for which features are locked/unlocked?

vercenta - October 30, 2018, 3:41 am

just find out what is accessing the memory of 703

Kufe - October 30, 2018, 3:46 am

(Oct 30, 2018 03:41 AM)John Doe 5726 Wrote: [\[CITE\]](#) So what is the problem if it does work?

What could that value be?

Does the program have an expiration date? Several plans for which features are locked/unlocked?

When it works all is fine. I'm not sure if there is any expiration date - probably not. I just can't figure out how it calculates this number.

(Oct 30, 2018 03:41 AM)Lost Doggy Wrote: [\[CITE\]](#) just find out what is accessing the memory of 703
How can I do that? I posted code in my first post, but the problem is that I don't know how app checks value if it's correct when it gets it.

John Doe 5726 - October 30, 2018, 3:52 am

(Oct 30, 2018 03:46 AM)Kufe Wrote: [\[CITE\]](#) When it works all is fine. I'm not sure if there is any expiration date - probably not. I just can't figure out how it calculates this number.

How can I do that? I posted code in my first post, but the problem is that I don't know how app checks value if it's correct when it gets it.

I'm not on x86 so I can't spin up a Windows VM and debug your app, so you want to figure out what the value is when the program already works?

Kufe - October 30, 2018, 3:58 am

Yes, I want to know how app does the check, so 3. returned web parameter (1st and 2nd are not important) is received (example: 1149) and then app does the check. If it's wrong number (example: any other number as 1149) it displays error, if it's correct number it displays Welcome message. And from looking the code it has to be generated by second part of HW ID (example 39573726000) - it's information from disk if I am correct (first part if generated by register MachineGuid value - but I changed that and app still worked while checking the returned number).

vercenta - October 30, 2018, 3:59 am

maybe 703 isn't that relevant lol?? doesn't seem to serve too much purpose of security
if the program accepted 703 two weeks ago and it does still today then it's probably fine

Kufe - October 30, 2018, 4:01 am

(Oct 30, 2018 03:59 AM)Lost Doggy Wrote: [\[CITE\]](#) maybe 703 isn't that relevant lol?? doesn't seem
to serve too much purpose of security
if the program accepted 703 two weeks ago and it does still today then it's probably fine
Each computer gets different number returned. It's based on sent HWID.

vercenta - October 30, 2018, 4:14 am

do 0-65535 until it works ;)

John Doe 5726 - October 30, 2018, 4:15 am

(Oct 30, 2018 04:14 AM)Lost Doggy Wrote: [\[CITE\]](#) do 0-65535 until it works ;)
I considered on advising this but then realized it wouldnt be so easy to see if it worked,
automatically, considering it has a GUI.

Kufe - October 30, 2018, 4:23 am

Well that is how I got to the correct numbers now, but it takes too long and I was hoping someone
would be able to figure out from decompiled code how it's checked and I would be able to get that
number easier. :)

vercenta - October 30, 2018, 4:35 am

lol then nop the function that retrieves the HWID and write the memory of a HWID you know returns
703

Kufe - October 30, 2018, 4:57 am

If I would only know how to do that. :) Max I came to is to decompile the code from app but can't
manage to figure out how it checks the number.

AbakBarama - October 30, 2018, 6:10 am

Solved.

```
Code char pszID[]="9A979599C66D9D9D996E9F9A20203356300";  
int nIndex, nChecksum=0;  
for (nIndex=24; nIndex<strlen(pszID); nIndex++)  
nChecksum=nChecksum+(pszID[nIndex]-'0')*nIndex;
```

Kufe - October 30, 2018, 7:51 am

Awesome, this is it. ?

Thanks alot AbakBarama, you saved me a lot of time. ?