Subject: new! ANTI VIRUS FALSE POSITIVE with Upp (GUI MT FileSel)
Posted by kohait00 on Mon, 09 May 2011 12:46:49 GMT
View Forum Message <> Reply to Message

running current (updated) freeav (avira) and try compile

reference/FileSelPreview with
GUI MT, MSC9, all static, without BLITZ

--> false positive: TR/Crypt.XPACK.Gen2.

compile withouth MT or in DEBUG does not yield the false positive.. i suppose its only MSC9 problem. didnt try with mingw though.

traced it down to be FileSel the problem. (make new empty CtrlLib project, GUI MT, put a FileSel in the app class, compile like above. thats all).

what can be done with it?

Subject: Re: new! ANTI VIRUS FALSE POSITIVE with Upp (GUI MT FileSel)
Posted by mirek on Mon, 09 May 2011 13:20:33 GMT
View Forum Message <> Reply to Message

kohait00 wrote on Mon, 09 May 2011 08:46running current (updated) freeav (avira) and try compile

reference/FileSelPreview with
GUI MT, MSC9, all static, without BLITZ

--> false positive: TR/Crypt.XPACK.Gen2.

compile withouth MT or in DEBUG does not yield the false positive.. i suppose its only MSC9 problem. didnt try with mingw though.

traced it down to be FileSel the problem. (make new empty CtrlLib project, GUI MT, put a FileSel in the app class, compile like above. thats all).

what can be done with it?

It sucks, but obviously, it is not FileSel problem, but freeave (avira) problem....

Maybe you should let them know, with exact steps to reproduce the problem?

Mirek

Subject: Re: new! ANTI VIRUS FALSE POSITIVE with Upp (GUI MT FileSel)
Posted by kohait00 on Mon, 09 May 2011 13:23:58 GMT
View Forum Message <> Reply to Message

yea, i know it's AV business. upp is out of guilty here. but FileSel was the part causing the false positive.

i really ask my self if they will care about this, upp is too small yet.. but ill do.. will send them an exe example so they can analyze it..

EDIT: just phoned avira. this is really bad, they only fix it for compiled exes. not generally, so that upp in general could profit from it. i'll try it anyway..am in contact with them..

Subject: Re: new! ANTI VIRUS FALSE POSITIVE with Upp (GUI MT FileSel)
Posted by mirek on Mon, 09 May 2011 14:43:07 GMT
View Forum Message <> Reply to Message

Hm, in theory, I would say that perhaps the code that is fetching icons from the system could be the culprit.... Maybe it would be worth to try to exlude it?

Subject: Re: new! ANTI VIRUS FALSE POSITIVE with Upp (GUI MT FileSel)
Posted by kohait00 on Mon, 09 May 2011 14:52:21 GMT
View Forum Message <> Reply to Message

that'd be great..is it an easy task should i try it or is it best any one with more indepth sight does it?

Subject: Re: new! ANTI VIRUS FALSE POSITIVE with Upp (GUI MT FileSel)
Posted by mirek on Mon, 09 May 2011 17:54:08 GMT
View Forum Message <> Reply to Message

kohait00 wrote on Mon, 09 May 2011 10:52that'd be great..is it an easy task should i try it or is it best any one with more indepth sight does it?

I bet you can. Comment out content of

virtual Image FileIconMaker::Make() const {

```
/* */
   return Null;
}
```

Mirek

Subject: Re: new! ANTI VIRUS FALSE POSITIVE with Upp (GUI MT FileSel)
Posted by kohait00 on Tue, 10 May 2011 07:16:05 GMT
View Forum Message <> Reply to Message

i tried it, unfort. this didnt help.
is there anything else 'potentially' unsafe in FileSel?

Subject: Re: new! ANTI VIRUS FALSE POSITIVE with Upp (GUI MT FileSel)
Posted by kohait00 on Tue, 10 May 2011 08:06:18 GMT
View Forum Message <> Reply to Message

i found the reason why it's ringing a false positive:

NetNode.cpp

::WNetOpenEnum()
::WNetOpenRessource()

as soon as one of theese is present, boom...

but it's a problem, quite a huge one. theese are Windows Functions. we can't change the code in any way.

i'll try to contact avira again.

Subject: Re: new! ANTI VIRUS FALSE POSITIVE with Upp (GUI MT FileSel)
Posted by kohait00 on Tue, 07 Jun 2011 09:43:53 GMT
View Forum Message <> Reply to Message

it's a month now and i havent heared anything from these guys over at antivir. no changes arrived with any updates, though i have sent them some example exes that trigger the error as well.

so any of those WNet* functions in NetNode are triggering the fals e positive. is there a possible workaround for that?

has any of you guys experienced the same problems? (with free av for windows)
