Subject: Is EasyHook or any other hooking library supported by U++ ?
Posted by smartytwiti on Tue, 08 Jan 2013 10:49:51 GMT
View Forum Message <> Reply to Message

We making a security software and we plan to use some Hooking library like EasyHook or perhaps some commercial one...
those libs are supported with VC++ and other IDE but we want to use U++ only to improve productivity.

Is it supported by U++ ?
There is any one has done some Hooking task using U++?
There is a native library built on U++?

PS: I'm newer to U++ and this is my first thread.

Subject: Re: Is EasyHook or any other hooking library supported by U++ ?
Posted by dolik.rce on Tue, 08 Jan 2013 12:12:56 GMT
View Forum Message <> Reply to Message

smartytwiti wrote on Tue, 08 January 2013 11:49We making a security software and we plan to use some Hooking library like EasyHook or perhaps some commercial one...
those libs are supported with VC++ and other IDE but we want to use U++ only to improve productivity.

Is it supported by U++ ?
There is any one has done some Hooking task using U++?
There is a native library built on U++?

PS: I'm newer to U++ and this is my first thread.

Hi smartytwiti

Welcome to the forum

I'm not a windows programmer, but from the quick glance at the EasyHook webpage, it seems that there should be no problem using it. It is just a bunch of DLLs and a header file, so it should work just as any other library, right?

I'm not aware about anyone using this, actually I never even heard of it However, I'm quite curious, could you please explain in few words what it is good for? There are chances that other ways to do the same things in more portable manner exist with U++

Best regards,
Honza

Subject: Re: Is EasyHook or any other hooking library supported by U++ ?
Posted by smartytwiti on Tue, 08 Jan 2013 13:03:16 GMT
View Forum Message <> Reply to Message

Thanks for reply
Well, EasyHook or any hook library its make hooking on windows much easier than ever,
Hooking API on windows is used by Antivirus to debug, view API call, Virtualize and Sandbox any running application.
When your application for example create a file(txt,exe...) its make a call to CreateFileW function on Windows kernel, so from that you can Hook this call Override itby returning INVALID_HANDLE_VALUE and execute your own function that's show "access denied " and in this way how works AV software..

It is just a bunch of DLLs and a header file, so it should work just as any other library
Glad to hear that, but when i make a tour on U++ i have seen some guys looking to how to add DLL to their project and have some issues with that..
In addition i have found this, but i can't get a clean way to iclude DLL file..
I don't know what's this DLi.. could anyone explain to me please?

Subject: Re: Is EasyHook or any other hooking library supported by U++ ?
Posted by zsolt on Tue, 08 Jan 2013 22:59:18 GMT
View Forum Message <> Reply to Message

.dli is just a way to simplify runtime loading and using dlls.
It is useful if you want to write a program, that loads libraries runtime. E.g. you want your program to work with several versions of a dll, but also without it.

See this link:
http://www.ultimatepp.org/srcdoc$Core$DLI$en-us.html

Subject: Re: Is EasyHook or any other hooking library supported by U++ ?
Posted by koldo on Wed, 09 Jan 2013 07:38:01 GMT
View Forum Message <> Reply to Message

Hello smartytwiti

Do not worry about DLL calls in Windows. They are ultra easy to be used. Just some ways:
- If you have the adecuate .lib file you can include them in the linking process
- You can use U++ DLI files.
- If you want low level direct control, you can call them directly. Here is the code of class Dl in U++/Bazaar/Functions4U library:

```
class Dl {
public:
 Dl::Dl() {
  hinstLib = 0;
```

```
}
Dl::~Dl() {
 if (hinstLib)
  if (FreeLibrary(hinstLib) == 0)
   throw Exc(t_("Dl cannot be released"));
}
bool Dl::Load(const String &fileDll) {
 if (hinstLib)
  if (FreeLibrary(hinstLib) == 0)
   return false;

 hinstLib = LoadLibraryEx(TEXT(fileDll), NULL, LOAD_IGNORE_CODE_AUTHZ_LEVEL);
 if (!hinstLib)
  return false;
 return true;
}
void *Dl::GetFunction(const String &functionName) {
 if (!hinstLib)
  return NULL;
 return (void *)GetProcAddress(hinstLib, functionName);
}
private:
 HINSTANCE hinstLib;
};
```

With Load() you open the DLL file and with GetFunction() you get the pointer to the function

---

Subject: Re: Is EasyHook or any other hooking library supported by U++ ?
Posted by smartytwiti on Wed, 09 Jan 2013 09:42:27 GMT
View Forum Message <> Reply to Message

@koldo:+1 your answer helped me!
My regards.

Subject: Re: Is EasyHook or any other hooking library supported by U++ ?
Posted by koldo on Wed, 09 Jan 2013 14:50:43 GMT
View Forum Message <> Reply to Message

Of course this is low level and not adequate for importing lots of functions but it always works .