

Forum: [Hack Forums](#)

Thread: [Best place to learn malware coding/reversing in C/C++](#)

F-Nuke - June 20, 2018, 6:29 pm

What is the best place to learn malware coding/reversing in C/C++? Forums, general resources, books, etc., anything is fine really.

Resources:

<https://tuts4you.com/> (Courtesy: [aeiro](#))

<http://185.62.190.110/> (Courtesy: [Toxcique](#))

<https://hackforums.net/showthread.php?tid=5852115&pid=57264953#pid57264953> (Courtesy: [Mr. Kim](#))

Thank you.

aeiro - June 20, 2018, 7:04 pm

(Jun 20, 2018 06:29 PM)F-Nuke Wrote: [\[CITE\]](#) What is the best place to learn malware coding/reversing in C/C++? Forums, general resources, books, etc., anything is fine really.

Thank you.

If you're looking for a forum who's sole purpose is reversing <https://tuts4you.com/> is the spot.

F-Nuke - June 21, 2018, 4:02 am

(Jun 20, 2018 07:04 PM)aeiro Wrote: [\[CITE\]](#) If you're looking for a forum who's sole purpose is reversing <https://tuts4you.com/> is the spot.

I've known tuts4you for a while. Amazing resources there.

Sajuuk - June 21, 2018, 7:22 pm

(Jun 21, 2018 04:02 AM)F-Nuke Wrote: [\[CITE\]](#) I've known tuts4you for a while. Amazing resources there.

Over the years, I've seen this question pop up time and time again. In recent days, I've been reading over the responses to these questions. I'll tell you now that my response will be biased, but I'll try to keep it as neutral as I possibly can.

Tuts4you does have an abundance of extremely detailed documents for almost if not every aspect of malware and it's (efficient) development. But, from my perspective, also taking into account the years I've had to review the information given, there is no one true resource that covers everything that can be done. That includes everything, including websites, books, and guides.

And that alone is the reason why quite a few people say programming skill comes from the person's style. And the person's style usually comes from how they learned the craft. That's how, and what, of course. It comes with time, but it will only come with time if the person dedicates that time to learning and practicing.

All of that time cannot be spent in one book alone. Different people learn better under different circumstances. Different people have different styles of coding (structure-wise for a simple example). Delve into varying topics. They don't all have to be about a specific part of the process, not do they have to be relative to malware at all.

tl;dr Tuts4you is the best resource from what I've found. It's essentially a goldmine of documents that cover a wide array of diverse topics across a large number of languages and systems.

F-Nuke - June 22, 2018, 2:57 am

(Jun 21, 2018 07:22 PM)Sajuuk Wrote: [\[CITE\]](#) Over the years, I've seen this question pop up time and time again. In recent days, I've been reading over the responses to these questions. I'll tell you now that my response will be biased, but I'll try to keep it as neutral as I possibly can.

Tuts4you does have an abundance of extremely detailed documents for almost if not every aspect of malware and it's (efficient) development. But, from my perspective, also taking into account the years I've had to review the information given, there is no one true resource that covers everything that can be done. That includes everything, including websites, books, and guides.

And that alone is the reason why quite a few people say programming skill comes from the person's style. And the person's style usually comes from how they learned the craft. That's how, and what, of course. It comes with time, but it will only come with time if the person dedicates that time to learning and practicing.

All of that time cannot be spent in one book alone. Different people learn better under different circumstances. Different people have different styles of coding (structure-wise for a simple example). Delve into varying topics. They don't all have to be about a specific part of the process, not do they have to be relative to malware at all.

tl;dr Tuts4you is the best resource from what I've found. It's essentially a goldmine of documents that cover a wide array of diverse topics across a large number of languages and systems.
I agree. Tuts4you is pretty awesome. But it leans more towards the reversing scene.

Do you happen to know of any forums of sorts where one can hold discussions solely on malware development/analysis?

Toxicique - June 22, 2018, 2:57 am

This webpage is also great:

<http://185.62.190.110/>

F-Nuke - June 22, 2018, 3:21 am

(Jun 22, 2018 02:57 AM)Toxicique Wrote: [\[CITE\]](#) This webpage is also great:

<http://185.62.190.110/>

This looks great! Thanks for sharing. :)

Mr. Kim - June 25, 2018, 1:51 pm

Check out this channel: [link](#)

It has all kinds of playlists on arm assembly, x86 assembly, rootkit development, and a lot of other awesome shit. If you learn more from listening than reading, these can be a godsend. They're very high quality and 100% free. In addition to that channel I've come across all kinds of various lectures on you tube over the years. Below are some of the best ones imo.

Stuxnet analysis - Bruce Dang (Microsoft) - [link](#)

Inside the Mac OS X Kernel - "Lucy" - [link](#)

Unleashing An x86 Design Flaw Allowing Universal Privilege Escalation - Christopher Domas - [link](#)

Breaking the x86 Instruction Set - Christopher Domas - [link](#)

As far as books go:

Windows Internals (any edition, 7 or 6 ideally) - Various Microsoft people

The Rootkit Arsenal - Bill Blunden

Rootkits: Subverting the Windows Kernel - Greg Hoglund & James Butler

For source code to study, presuming windows is your main focus take a look at [the windows research kernel](#) as well as [the reactos source](#)

Lemme know if you have any questions ?

HiddenEyE - June 27, 2018, 2:17 am

nice post mates. but i still believe in old new things.

Mr. Kim - June 29, 2018, 5:29 am

(Jun 27, 2018 02:17 AM)HiddenEyE Wrote: [\[CITE\]](#) nice post mates. but i still believe in old new things.

What do you mean by this?

int - June 29, 2018, 11:54 am

for reversing malware, I liked that guy max on youtube. I looked for a link, didn't find it. They aren't step by step tutorials, but they show you the tools that are needed for reversing.

SteamedHams - June 29, 2018, 4:56 pm

You can add rohitab.com to the list, but at this time it is a bit of a ghost town.

inyourmemory - June 30, 2018, 9:50 am

Best to start reading some malware analysis blogs and sites, they often explain detailly how the malware works and what mistakes were made and even sometimes include code snippets.

Then your usual malware sources and classic ones line Zeus.

Kali_Shadow - July 2, 2018, 5:52 am

good share bro , Thanks for the links ... !!

Sparkling Jack - July 11, 2018, 2:00 am

In terms of malware coding tech, I recommend this website.
w www.malwaretech.com

It has many recent malware coding techniques and methods.
It will be a good choice for understanding how malwares work.

Luulz - July 17, 2018, 3:13 pm

Implying you want to focus on Windows

Unknowncheats, even if it is most likely centered around game hacking, will give you indepth knowledge for Rootkits ideas, and stealthy behaviour.

Then, the book you need to READ INTENSIVELY is "Windows Internal". 7th edition is focused around w10, but you can still find on google the 6th edition which will be faaar enough if you're beginning in that section.

BigDawgAustin - July 6, 2021, 2:29 am

Thanks So Much
I'll Be Sure To Check This Out