

Forum:[Hack Forums](#)

Thread: [Lycosidae - Modern Anti Debug](#)

donovanranda - October 17, 2019, 6:57 am

github.com/lurumdare/Lycosidae

Bypass ScyllaHide

Features

- Import no leak
- Strings no leak

Paskowsky - October 17, 2019, 7:47 am

(Oct 17, 2019 06:57 AM)donovanranda Wrote: [\[CITE\]](#) github.com/lurumdare/Lycosidae

Bypass ScyllaHide

Features

- Import no leak
- Strings no leak

Working link : <https://github.com/lurumdare/Lycosidae>

I dont know if this is your code, but it's not bad. I've looked at source code and basically you are restoring hooked functions from scyllahide that is "new" and all the functions you call are called by hash which is something malwares and or shellcodes do since 1999 ? ? .

However a reverser looking at code will notice, maybe not on first run, that his plugin isn't working and just patch the code so crc check to compare functions always returns true.
That's a solution that crossed my mind just now.

A layer of obfuscation would decrease probabilities of this happening so it's still a good release ?

Regards,
Paskowsky ?

SKIDROOTKIT - October 17, 2019, 12:23 pm

This won't do anything. You can easily work on this.

donovanranda - October 18, 2019, 10:05 am

(Oct 17, 2019 07:47 AM)Paskowsky Wrote: [\[CITE\]](#) I dont know if this is your code, but it's not bad. I've looked at source code and basically you are restoring hooked functions from scyllahide that is "new" and all the functions you call are called by hash which is something malwares and or shellcodes do since 1999 ? ? .

However a reverser looking at code will notice, maybe not on first run, that his plugin isn't working and just patch the code so crc check to compare functions always returns true.
That's a solution that crossed my mind just now.

A layer of obfuscation would decrease probabilities of this happening so it's still a good release ?

Regards,
Paskowsky ?
Yes. It is my code.

Read VM_Manul.md

if you add virtualization,
it will be hard for the reverser

dracx - October 19, 2019, 2:53 am

(Oct 18, 2019 10:05 AM)donovanranda Wrote: [\[CITE\]](#) Yes. It is my code.

Read VM_Manul.md

if you add virtualization,
it will be hard for the reverser
may I ask how would virtualization help?

SKIDROOTKIT - October 19, 2019, 2:09 pm

(Oct 19, 2019 02:53 AM)dracx Wrote: [\[CITE\]](#) may I ask how would virtualization help?

It's just a layer of obscurity. Any decent reverse engineer should be able to reverse virtual handlers that lead to the devirtualization of vm opcodes.

binbus - October 19, 2019, 10:38 pm

(Oct 19, 2019 02:09 PM)SKIDROOTKIT Wrote: [\[CITE\]](#) It's just a layer of obscurity. Any decent reverse engineer should be able to reverse virtual handlers that lead to the devirtualization of vm opcodes.

Then why have you never done it?

SKIDROOTKIT - October 19, 2019, 10:44 pm

(Oct 19, 2019 10:38 PM)binbus Wrote: [\[CITE\]](#) Then why have you never done it?

Wdym? This is a general thing. Reversing a virtualization system isn't difficult in theory. The only thing that stands in its way is more obscurity.. obfuscation, encryption, etc.

smutnagab - October 20, 2019, 2:26 pm

(Oct 19, 2019 10:38 PM)binbus Wrote: [\[CITE\]](#) Then why have you never done it?There's no need to get emotional and attack him out of the blue, he's just stating facts. I don't see how what he has said is "offensive" and justifies the response you gave him. The point of a forum like HackForums is to share knowledge!

A layer of virtualisation would merely be more obscurity which results in more work for the reverse-engineer in order to get the information they desire, but if the reverse-engineer is skilled and determined enough, they will inevitably get through it all.

If the virtualisation is custom for each use-case (e.g. different virtual operation codes being translated with changes in the algorithms for the conversion, etc.) then it can be tiresome and ware the reverse-engineer out if they have to reverse-engineer many binaries apart of the same software package using a virtualisation layer, but even this would still be trivial if they were skilled and determined enough to get the task at hand completed. It would merely take them more time to get the information they desire to extract from the software.

binbus - *October 20, 2019, 9:02 pm*

(Oct 19, 2019 10:44 PM)SKIDROOTKIT Wrote: [\[CITE\]](#) Wdym? This is a general thing. Reversing a virtualization system isn't difficult in theory. The only thing that stands in its way is more obscurity.. obfuscation, encryption, etc.

Do it then

Skid

[warn]

vertox - *October 21, 2019, 8:46 pm*

(Oct 20, 2019 09:02 PM)binbus Wrote: [\[CITE\]](#) Do it then

Skid

[warn]

don't rek me now bro

donovanranda - *October 28, 2019, 11:29 pm*

add few checks

check project on github