

Forum: [Hack Forums](#)

Thread: [Windows Process Injection Toolkit](#)

n00bmk - July 27, 2018, 4:16 am

So, I decided to make my own multi-injection kit which will utilize every conceivable method of process injection.

Its purely coded in C#, but may be widened to C/C++ in the future if needed for more generic methods...

Anyways, here it is: <https://github.com/m4mm0n/WinPIT>

And as always, please do make issue reports if bugs are found - I know the last added injector is buggy and unstable...

Also, everything gets logged - check the sources ;)

NTW5B - July 27, 2018, 2:04 pm

(Jul 27, 2018 04:16 AM)n00bmk Wrote: [\[CITE\]](#) So, I decided to make my own multi-injection kit which will utilize every conceivable method of process injection.

Its purely coded in C#, but may be widened to C/C++ in the future if needed for more generic methods...

Anyways, here it is: <https://github.com/m4mm0n/WinPIT>

And as always, please do make issue reports if bugs are found - I know the last added injector is buggy and unstable...

Also, everything gets logged - check the sources ;)

Could you please add a ReplacePE?? (Replace Process)

This is one of the Best thing's I've seen online...

In C/C++, use C for Stability

For the C/C++, Don't use LoadLibrary/ProcAdress to hide imports, The stub will get flagged as a packer EVERYWHERE

Search: 50c863f238d8328804d7e96e583cf1d2c707419184937ae68cb038a71f8bc568

On hybrid-analysis and It gets flagged as "kryptor 6" while on YODAS PROTECTOR, I only checked "Hide Imports"

it uses LoadLibrary/ProcAdress

Plus, Some of those stuff aren't needed, but No matter what, FALCON/Cylance will detect anything

Just use C/C++ antis and You'll be done..

HFDone - July 29, 2018, 11:13 am

"Credits are due where credits are due, no greets and no regrets!"

Add Credit <https://github.com/Washi1337/AsmResolver>

dont know why you using it

your ManualMap is just for 64bit

<https://github.com/vmcall/loadlibrary/blob/master/Injection/ManualMap.cs> ?=

<https://github.com/m4mm0n/WinPIT/blob/master/Injectors.ManualMap/Injector.cs>

...

Washi - July 29, 2018, 2:19 pm

Great that someone is using my library!

However, I kindly ask you to obey the license terms that I set for using it. AsmResolver is released under the LGPLv3 license, which essentially means that you are free to use it anywhere, so long you include the original copyright and license notices of the library, as well as a reference to the original source, and state any changes that you have made to the library.

For more information, read:

<https://github.com/Washi1337/AsmResolver/blob/master/LICENSE.md>

Or use the TL;DR for an easy to read list of all conditions that you should obey.

[https://tldrlegal.com/license/gnu-lesser-general-public-license-v3-\(lgpl-3\)](https://tldrlegal.com/license/gnu-lesser-general-public-license-v3-(lgpl-3))

n00bmK - July 29, 2018, 4:25 pm

Apologiez, honestly thought I had added you to the credits - but will be fixed :)