

Forum:[Hack Forums](#)

Thread: [Process hollowing in Win 10](#)

invisible_hack2 - May 22, 2020, 3:48 pm

I would like to know if this technique is still valid in windows 10 and if it continues to hide the suspended process since now you can see all the suspended processes in windows 10.

which is a good technique to hide the process apart from process hollowing and injection dll?

thank you

Sinistros - May 23, 2020, 8:42 am

(May 22, 2020 03:48 PM)invisible_hack2 Wrote: [\[CITE\]](#) I would like to know if this technique is still valid in windows 10 and if it continues to hide the suspended process since now you can see all the suspended processes in windows 10.

which is a good technique to hide the process apart from process hollowing and injection dll?

thank you

Hello, i guess the best dll injection is manual mapping, it is the most hidden technique.

Chameleon - May 23, 2020, 10:00 am

(May 23, 2020 08:42 AM)Sinistros Wrote: [\[CITE\]](#) Hello, i guess the best dll injection is manual mapping, it is the most hidden technique.

Oh darn, i was just about to say that haha.. good one brother

Jean-Jacques Rousseau - May 24, 2020, 5:56 am

(May 23, 2020 08:42 AM)Sinistros Wrote: [\[CITE\]](#) Hello, i guess the best dll injection is manual mapping, it is the most hidden technique.

Depends on how youre doing it.

OP: what do you mean by suspended process? It i resumed once mapping is done.

invisible_hack2 - May 27, 2020, 11:26 am

(May 24, 2020 05:56 AM)Supercut Wrote: [\[CITE\]](#) Depends on how youre doing it.

OP: what do you mean by suspended process? It i resumed once mapping is done.

Correct, it's resumed, i'm not tested this technique yet, i don't know if it works in win 10

Jean-Jacques Rousseau - May 27, 2020, 12:06 pm

(May 27, 2020 11:26 AM)invisible_hack2 Wrote: [\[CITE\]](#) Correct, it's resumed, i'm not tested this technique yet, i don't know if it works in win 10

Of course it works. It is unpatchable.

Zanthir - May 27, 2020, 4:15 pm

Ive tested it works fine !

SIM-3466371 - June 19, 2020, 3:37 pm

(May 22, 2020 03:48 PM)invisible_hack2 Wrote: [\[CITE\]](#) I would like to know if this technique is still

valid in windows 10 and if it continues to hide the suspended process since now you can see all the suspended processes in windows 10.

which is a good technique to hide the process apart from process hollowing and injection dll?

thank you

Yes, it's still working in all windows versions.

Because this technique uses api calls and it's not a vulnerability.

If you have equal or more privileges than target process, why not??

Most AV will detect it, specially api calls like Get/setThreadContext, createreomotethread, WriteMemory