

Forum:[Hack Forums](#)

Thread: [VM / Sandboxie Detector](#)

ac3n34d_X - July 20, 2018, 2:07 pm

Can Anyone Write Me a Simple Function to Detect VM or Sandboxie and Other Debuggers... With A Bool Return Value in VB.Net Please. I Know The Language Is Old But I Just Wanna Test Out Something ?

Thanks In Advance ? ?

NYANxCAT - July 20, 2018, 8:03 pm

Very basic project [not mine] <http://prntscr.com/k94chv>

download

<https://www.sendspace.com/file/z76z5k>

I hope you learn from it.

EDIT:-

Quote:I Know The Language Is Old there is no such this as old language. and btw c# is 1 year older than vb.net

Vyxn - July 20, 2018, 10:19 pm

(Jul 20, 2018 02:07 PM)ac3n34d_X Wrote: [\[CITE\]](#) I Know The Language Is Old But I Just Wanna Test Out Something ?

VB6 is old, VB.NET is new.

InterGalactic - August 27, 2018, 4:54 am

Why you just dont check for running processes and then return a the value if something found?
Just saying :P Im bored to code it.

gigajew - September 13, 2018, 7:57 pm

lunacyrcus - October 1, 2018, 10:53 pm

(Jul 20, 2018 02:07 PM)ac3n34d_X Wrote: [\[CITE\]](#) Can Anyone Write Me a Simple Function to Detect VM or Sandboxie and Other Debuggers... With A Bool Return Value in VB.Net Please. I Know The Language Is Old But I Just Wanna Test Out Something ?

Thanks In Advance ? ?

search "usermode hook detection" on google

oxidebuffalo - October 3, 2018, 9:17 am

All you need to do is reverse-engineer some sandboxes like Sandboxie to identify some GUIDs. A simple one would be checking for "SbieDll.dll" which will be injected into the sandboxed process, or checking for the current user account the process is executing under the context of (e.g. Sandboxie spawns under another user account).

You can check for user-mode API hooks on certain routines as well, which is simple byte-comparison.

For anti-VM, you can check for GUIDs through enumeration of processes and registry. For anti-debugging in general, you can do a wide range of things from accessing the PEB fields to checking for kernel debugging support on the environment.