Forum:Hack Forums

Thread: WinXRunPE | 32-bit<>32-bit RunPE that works in ANY MODE! (x86, x64, AnyCPU)

gigajew - *November 27, 2018, 6:38 pm*

Finally went and spent a lot of time writing and researching using mainly Windbg, (that I cannot explain in words how much I love) and came up with this. It's a RunPE that can inject any 32-bit payload into any 32-bit process. On Windows 10. On a 64-bit system. In any build target (x86, x64, AnyCPU). It does not support relocations however. The reason I'm doing all this is because I'm working my way towards creating a fully functional x64<>x64 injector. But I need to read up some more.

As always I share my code with everyone for free, for educational purposes and for the greater good. Knowledge should be free to those who seek it.

Let me know what you think about it :)

Usage:
Spoiler (Click to View)

Sauce:
Spoiler (Click to View)

HFDone - *November 28, 2018, 1:48 am*

been here since 2014
Menalix mena runpe https://hackforums.net/showthread.php?tid=4432024

gigajew - *November 28, 2018, 7:28 pm*

(Nov 28, 2018 02:48 AM)HFDone Wrote: *[CITE]* been here since 2014
Menalix mena runpe https://hackforums.net/showthread.php?tid=4432024
This was aimed more at native executables. I just included menalix's net patch that was modified by me

gigajew - *December 1, 2018, 5:32 pm*

Please do check GitHub for updates: https://github.com/gigajew/WinXRunPE-x86_x64 which is also going to be my "private" edition

Menalix - *December 8, 2018, 9:14 pm*

nice release, look really smooth!

cryptoshell - *December 11, 2018, 7:13 am*

(Dec 1, 2018 06:32 PM)gigajew Wrote: *[CITE]* Please do check GitHub for updates: https://github.com/gigajew/WinXRunPE-x86_x64 which is also going to be my "private" edition
nice job bro
thanks for keeping it update

qurexhi - *January 2, 2019, 6:29 am*

Any Tutorial Brother??????????

onishn96 - *January 12, 2019, 4:48 am*

Hello, i m start debug and application work good.After i m building application and will start its open but doesn't work.