Forum:Hack Forums

Thread: To prove you fuckers wrong [64-Bit Injection]

iSam - *August 21, 2010, 9:13 pm*
64 bit injection into explorer.exe

[img]http://i36.[censored].com/2likcpy.png[/img]

birdy9 - *August 21, 2010, 9:18 pm*
tested it my self.

now awaiting brix to be shat by all the HF children.

Widow's Peak - *August 21, 2010, 9:20 pm*
Wait what's so special? A runpe was released with 64 bit injection a while back

babyvamp666 ? - *August 21, 2010, 9:22 pm*
what are you trying to prove that you coded a 64 bit runpe? oh really nice (sacarism).

superpriv5 - *August 21, 2010, 9:23 pm*
ITT: VB.NET and it's skid learners.

masterjippo - *August 21, 2010, 9:26 pm*
Is that code injection ? (inserting just a function)
or PE injection? (exe, dll) (and which)
also, is it a createprocess, unmap & remap new, or 2 PE's into same process?
lang?

iSam - *August 21, 2010, 9:28 pm*
(Aug 21, 2010 09:23 PM)superpriv5 Wrote: *[CITE]* ITT: VB.NET and it's skid learners.
ITT: skids that think i code in VB

Quote:Is that code injection ? (inserting just a function)
or PE injection? (exe, dll) (and which)
also, is it a createprocess, unmap & remap new, or 2 PE's into same process?

Its code injection into explorer.exe. I saw no previous examples of this.

(Aug 21, 2010 09:20 PM)camgaertner Wrote: *[CITE]* Wait what's so special? A runpe was released with 64 bit injection a while back
Lol. Thats not injection at all, just memory execution. Also, if it has a parameter for injection, DEP will stop it anyway. This is DEP bypass.

wacked2 - *August 22, 2010, 3:10 am*
Uhm so what?
it´s like the normal way just:
Compiling in x64
VirtualAllocEx(..,PAGE_EXECUTE_READWRITE) (DEP bypass super pri8)
?

or did there is just ONE extra step?

crimepack - *August 22, 2010, 4:25 am*
you are compiling in x64 mode lol its nothing special with that

to inject from 32bit to 64bit process is the hard part, this is still achievable by breaking out of wow64 environment in to a native x64 environment but this is certainly not what you did

so what you just proved is that you just figured out that you could compile your exe as x64 (which wont run on 32bit systems) so this thread is more of a fail rather than you getting the e-rep you wanted

when did you start coding C++ anyways? i thought you were one of those VB nuthuggers

babyvamp666 ? - *August 22, 2010, 5:24 am*
(Aug 22, 2010 04:25 AM)crimepack Wrote: [CITE] you are compiling in x64 mode lol its nothing special with that

to inject from 32bit to 64bit process is the hard part, this is still achievable by breaking out of wow64 environment in to a native x64 environment but this is certainly not what you did

so what you just proved is that you just figured out that you could compile your exe as x64 (which wont run on 32bit systems) so this thread is more of a fail rather than you getting the e-rep you wanted

when did you start coding C++ anyways? i thought you were one of those VB nuthuggers
True, but still you can find the Drive & if Progam Files(x86) Exicts its 64 bits else 32 bits so is how i do it but sometimes it fails ;(

crimepack - *August 22, 2010, 5:26 am*
(Aug 22, 2010 05:24 AM)babyvamp666 ? Wrote: [CITE] True, but still you can find the Drive & if Progam Files(x86) Exicts its 64 bits else 32 bits so is how i do it but sometimes it fails ;(
its pretty easy to determine if its executed on a x64 system or not, still i don't get your point what you are trying to say though

babyvamp666 ? - *August 22, 2010, 5:28 am*
(Aug 22, 2010 05:26 AM)crimepack Wrote: [CITE] its pretty easy to determine if its executed on a x64 system or not, still i don't get your point what you are trying to say though
64 bits sys have Progam Files (x86) and 32 bits not.

E: Maybe not on XP but on vis/seven.

Squirtle - *August 22, 2010, 5:55 am*
(Aug 21, 2010 09:22 PM)babyvamp666 ? Wrote: [CITE] what are you trying to prove that you coded a 64 bit runpe? oh really nice (sacarism).Some nice sacarism you got there,

CppSean - *August 22, 2010, 6:00 am*
So what you trying to get at bro?

crimepack - *August 22, 2010, 6:17 am*
(Aug 22, 2010 05:28 AM)babyvamp666 ? Wrote: [CITE] 64 bits sys have Progam Files (x86) and 32 bits not.

E: Maybe not on XP but on vis/seven.
yeah i'm aware of that, but how is your response related to my reply at all?

iSam - *August 22, 2010, 9:56 am*
I wasn't trying to get e-rep at all, and I told multiple people it was easy but they didn't believe me, so I posted here. Don't get butthurt. Also to detect 64 bit systems all u gotta do is detect WOW64. GetProcAddress(GetModuleHandle("kernel32.dll"), "IsWow64Process");

(Aug 22, 2010 04:25 AM)crimepack Wrote: [CITE] you are compiling in x64 mode lol its nothing special with that

to inject from 32bit to 64bit process is the hard part, this is still achievable by breaking out of wow64 environment in to a native x64 environment but this is certainly not what you did

so what you just proved is that you just figured out that you could compile your exe as x64 (which wont run on 32bit systems) so this thread is more of a fail rather than you getting the e-rep you wanted

when did you start coding C++ anyways? i thought you were one of those VB nuthuggers
Broseph half these fucks didn't even believe it was possible. Also I haven't coded in VB for a long ass time, only delphi + C/C++ now. I would just use a 32 bit executable to determine whether its being run in a 32/64 bit system then either execute a processes which injects into 32 bit explorer or 64 bit explorer.

wacked2 - *August 22, 2010, 10:53 am*
actually you also need to call IsWow64Process.

p@rdon - *August 22, 2010, 11:00 am*
Well I'm glad Sam finally proved that he is smart enough to change one setting in Visual Studio. This is sure to revolutionize malware everywhere.

SpK - *August 22, 2010, 11:04 am*
Wow, this is a revolution in malware progamming. /sarcasm

p@rdon - *August 22, 2010, 11:10 am*
(Aug 22, 2010 11:04 AM)SpK Wrote: [CITE] Wow, this is a revolution in malware progamming. /sarcasm
HEY FUCKER LOOK WHAT I CAN DO
[img]http://clip2net.com/clip/m51241/1282500744-clip-51kb.png[/img]
YEAH I'M COOL

wacked2 - *August 22, 2010, 11:12 am*
You shouldn´t be so mean.
Let´s give him a group hug. If he thinks this is something cool we shouldn´t criticize him. Spread the love

SpK - *August 22, 2010, 12:05 pm*
I lol'd at that one haha

t

ovelayer - *August 22, 2010, 4:50 pm*

umm wait i think i will slap my buttcheeks together for you..
i mean really..this isn't good this is just comicbook material