Forum:Hack Forums

Thread: [FREE & RUNTIME FUD] Lua Builder [REQUEST ADMIN|CHANGE DROPPED ICON|CUSTOMIZABLE]

mafia_man - *May 8, 2014, 9:01 am*

[img]http://imagizer.imageshack.us/a/img842/2356/ny8l.png[/img]

[img]http://imagizer.imageshack.us/a/img838/5183/s2co.png[/img]
[Video: https://www.youtube.com/watch?v=h6-j3vP02Ng]
Lua Builder is a combination of C#, C++, BlitzMax and Lua itself.

Stub
Size: 510kB

It's written in BlitzMax and C++, and uses lua for your applications.
There are two stubs: gui and console for debugging lua code.

It's currently fud both runtime and scantime.

Builder
Builder is written in C#, and I included 3 binaries written in BlitzMax:encrypter.exe - Encrypts given data (I was to lazy to implement random number generator, which my stub uses)

resadd.exe - Adds resource to given executable

resicon.exe - Changes icon of given executable (not used yet)

Scans of builder, binaries and stubs
ClamAV (PUA.Win32.Packer.MingwGcc-2) is a false-positive.» Builder @ VirusTotal.com

» Stub (with crypter stub code and bound virus and fake installer) @ RazorScanner.com

» encrypter.exe @ VirusTotal.com

» resadd.exe @ VirusTotal.com

» resicon.exe @ VirusTotal.com

[img]http://imageshack.com/a/img843/6347/fg86.png[/img]

How to get it? It's only available for L33t, Ub3r, HF Staff and 3P1C.
And I can also make exceptions for some normal users, with good reputation.

I don't want some random skid upload stubs to virustotal.com, or shit site like that.
Just send me message here, on HF. ?

[img]http://imagizer.imageshack.us/a/img845/5326/4yl1.png[/img]

You can extern most win32 functions (if not all), because I am not using pure lua but LuaJIT. Read about it » here «

Those are available from my stub:
View functions (Click to View)Function fromcstring(int memoffset)
Description: Converts one byte sized string from specified memory offset and returns it to lua.
Returns: string

Function fromwstring(int memoffset)
Description: Converts 2 byte sized string from specified memory offset and returns it to lua.
Returns: string

Function tocstring(string string)
Description: Converts lua string to one byte sized string, and returns it address.
Returns: int

Function towstring(string string)
Description: Converts lua string to 2 byte sized string, and returns it address.
Returns: int

Function savememtofile(string filepath, int memoffset, int size)
Description: Reads data from specified memoffset, and writes it to file.
Returns: int

Function getresource(string resname, string restype, int reslangid, int hModule)
Description: Gets pointer to specified resource in hModule,
if hModule is set to 0, current executable hModule is used.
Returns nil if resource doesn't exist.
Returns: int/nil

Function addresource(string filepath, string resname, string restype, int reslangid, int memoffset, int size)
Description: Adds resource to specified file.
Returns: nil

Function changeicon(string filepath, string iconpath)
Description: Sets icon of file.
Returns: nil

Function me_setkey(string key, int encryptionpasses)
Description: Sets key for encryption/decryption.
Returns: nil

Function me_encrypt(int memoffset, int size)
Description: Encrypts/Decrypts given memory.
Returns: nil

Function me_encryptstring(string string)
Description: Encrypts string and returns it as base64 encrypted string.
Returns: string

Function me_decryptstring(string string)
Description: Decrypts base64 encrypted string.
Returns: string

Function input()
Description: Waits for console input, and returns it.
Returns: string

Function getversionex(int memoffset)
Description: http://msdn.microsoft.com/en-us/library/windows/desktop/ms724451(v=vs.85).aspx
Returns: int

Function gettokeninformation(int tokenHandle, int tokenInformationClass, int tokenInformation, int tokenInformationLength, int returnLength)
Description: http://msdn.microsoft.com/en-us/library/windows/desktop/aa446671(v=vs.85).aspx
Returns: int

Function getcurrentprocess()
Description: http://msdn.microsoft.com/en-us/library/windows/desktop/ms683179(v=vs.85).aspx
Returns: int

Function openprocesstoken(int processHandle, int desiredAccess, int tokenHandle)
Description: http://msdn.microsoft.com/en-us/library/windows/desktop/aa379295(v=vs.85).aspx
Returns: int

Function terminate()
Description: Terminates application.

Function getdir()
Description: Returns current directory.
Returns: string

Function getappargscount()

Description: Returns argument count.
Returns: int

Function getapparg(int argid)
Description: Returns specified argument id value.
Returns: string

Function getlasterror()
Description: http://msdn.microsoft.com/en-us/library/windows/desktop/ms679360(v=vs.85).aspx
Returns: int

Function shellexecute(int hwnd, string lpOperation, string lpFile, string lpParameters, string lpDirectory, int nShowCmd)
Description: http://msdn.microsoft.com/en-us/library/windows/desktop/bb762153(v=vs.85).aspx
Returns: int

Function createprocess(string lpApplicationName, string lpCommandLine, int lpProcessAttributes, int lpThreadAttributes, int bInheritHandles, int dwCreationFlags, int lpEnvironment, int lpCurrentDirectory, int lpStartupInfo, int lpProcessInformation)
Description: http://msdn.microsoft.com/en-us/library/windows/desktop/ms682425(v=vs.85).aspx
Returns: int

Function getint(int memoffset)
Description: Returns integer (4 bytes) from specified memory offset.
Returns: int

Function getshort(int memoffset)
Description: Returns short (2 bytes) from specified memory offset.
Returns: int

Function getbyte(int memoffset)
Description: Returns byte from specified memory offset.
Returns: int

Function setint(int memoffset, int integer)
Description: Sets integer (4 bytes) at specified memory offset.

Function setshort(int memoffset, int short)
Description: Sets short (2 bytes) at specified memory offset.

Function setbyte(int memoffset, int byte)
Description: Sets byte at specified memory offset.

Function memfree(int memoffset)
Description: Frees memory at specified offset.

Function memcopy(int dstmem, int srcmem, int count)
Description: Copies bytes from source to destination.

Function memalloc(int count)
Description: Allocates specified amount of memory and returns memory offset to allocated memory.
Returns: int

Function getthreadcontext(int hThread, int lpContext)
Description: http://msdn.microsoft.com/en-us/library/windows/desktop/ms679362(v=vs.85).aspx
Returns: int

Function virtualprotectex(int hProcess, int lpAddress, int dwSize, int flNewProtect, int lpflOldProtect)
Description: http://msdn.microsoft.com/en-us/library/windows/desktop/aa366899(v=vs.85).aspx
Returns: int

Function writeprocessmemory(int hProcess, int lpBaseAddress, int lpBuffer, int nSize, int lpNumberOfBytesWritten)
Description: http://msdn.microsoft.com/en-us/library/windows/desktop/ms681674(v=vs.85).aspx
Returns: int

Function setthreadcontext(int hThread, int lpContext)
Description: http://msdn.microsoft.com/en-us/library/windows/desktop/ms680632(v=vs.85).aspx
Returns: int

Function resumethread(int hThread)
Description: http://msdn.microsoft.com/en-us/library/windows/desktop/ms685086(v=vs.85).aspx
Returns: int

DaPiranha - *May 8, 2014, 9:04 am*
Finally, you released it hahaha, awesome stuff bro!

100% legit guy, deserves my vouch, very hard working and provides HQ stuff!

The Undertaker - *May 8, 2014, 9:10 am*
Can I have the link? I use http://fuckingscan.me/index.php

zaher7777 - *May 8, 2014, 11:21 am*
can u send me link to your crypte i use nodistribute.com

xBrokenSoul - *May 8, 2014, 2:34 pm*
Can I have a download link please? PM Me, thanks in advance ?

mafiaanonymous - *May 8, 2014, 10:09 pm*
Can Download Link Plasee , pm me , Thank you bro :D

4saken - *May 9, 2014, 3:46 am*
could you send me the download link? would love to get this.

Thanks :)

Ghrulx - *May 9, 2014, 4:05 am*
Could i get a download link? Kindly appreciated mate! Thank you for the hard work and dedication :3

Mr. Miyagi - *May 9, 2014, 4:14 am*
PMing you now OP, I would like to check this out.

Crizzybee - *June 4, 2014, 7:03 pm*
Looks great to use. Can I have the download link, please?
I'm currently use 'ResHacker', which is good but it's inconvenience than yours.

mafia_man - *June 5, 2014, 2:14 am*
It's not FUD anymore, only private stubs. I do not release them to public.