Vagaa协议分析

-----------------moonflow 2012.9.10

粗略记录下vagaa连接中的rc4加密:

.text:00473B10 sub\_473B10 proc near ; CODE XREF: sub\_413070+12p

.text:00473B10 ; sub\_41BE40+6Cp ...

.text:00473B10

.text:00473B10 var\_24 = dword ptr -24h

.text:00473B10 var\_20 = dword ptr -20h

.text:00473B10 var\_1C = dword ptr -1Ch

.text:00473B10 var\_18 = dword ptr -18h

.text:00473B10 var\_14 = dword ptr -14h

.text:00473B10 var\_10 = dword ptr -10h

.text:00473B10 var\_C = dword ptr -0Ch

.text:00473B10 var\_8 = dword ptr -8

.text:00473B10 var\_4 = dword ptr -4

.text:00473B10 arg\_0 = dword ptr 4

.text:00473B10

.text:00473B10 sub esp, 24h

.text:00473B13 mov eax, dword\_64AA84

.text:00473B18 mov [esp+24h+var\_4], eax

.text:00473B1C mov eax, [esp+24h+arg\_0]

.text:00473B20 test eax, eax

.text:00473B22 jz short loc\_473B40

.text:00473B24 mov ecx, [eax]

.text:00473B26 mov edx, [eax+4]

.text:00473B29 mov [esp+24h+var\_24], ecx

.text:00473B2C mov ecx, [eax+8]

.text:00473B2F mov [esp+24h+var\_20], edx

.text:00473B33 mov edx, [eax+0Ch]

.text:00473B36 mov [esp+24h+var\_1C], ecx

.text:00473B3A mov [esp+24h+var\_18], edx

.text:00473B3E jmp short loc\_473B68 ; RC4加密

.text:00473B40 ; ---------------------------------------------------------------------------

.text:00473B40

.text:00473B40 loc\_473B40: ; CODE XREF: sub\_473B10+12j

.text:00473B40 push esi

.text:00473B41 call ds:GetTickCount

.text:00473B47 imul eax, 1FDh

.text:00473B4D push eax ; unsigned int

.text:00473B4E call \_srand

.text:00473B53 add esp, 4

.text:00473B56 xor esi, esi

.text:00473B58

.text:00473B58 loc\_473B58: ; CODE XREF: sub\_473B10+55j

.text:00473B58 call \_rand

.text:00473B5D mov byte ptr [esp+esi+28h+var\_24], al

.text:00473B61 inc esi

.text:00473B62 cmp esi, 10h

.text:00473B65 jl short loc\_473B58

.text:00473B67 pop esi

.text:00473B68

.text:00473B68 loc\_473B68: ; CODE XREF: sub\_473B10+2Ej

.text:00473B68 mov ecx, dword\_6427B4 ; RC4加密

.text:00473B6E mov eax, dword\_6427B0

.text:00473B73 mov edx, dword\_6427B8

.text:00473B79 push 1

.text:00473B7B push 0

.text:00473B7D mov [esp+1Ch], ecx

.text:00473B81 mov [esp+18h], eax

.text:00473B85 mov eax, dword\_6427BC

.text:00473B8A lea ecx, [esp+8]

.text:00473B8E push 20h

.text:00473B90 push ecx

.text:00473B91 mov [esp+28h], edx

.text:00473B95 mov [esp+2Ch], eax

.text:00473B99 call sub\_4739B0

.text:00473B9E mov ecx, [esp+34h+var\_4]

.text:00473BA2 call sub\_5799BF

.text:00473BA7 add esp, 34h

.text:00473BAA retn

.text:00473BAA sub\_473B10 endp

.data:006427B0 dword\_6427B0 dd 318DB06Fh ; DATA XREF: sub\_473B10+5Er

.data:006427B4 dword\_6427B4 dd 0CA9423DCh ; DATA XREF: sub\_473B10:loc\_473B68r

.data:006427B8 dword\_6427B8 dd 18BCF62Dh ; DATA XREF: sub\_473B10+63r

.data:006427BC dword\_6427BC dd 0F45807A0h ; DATA XREF: sub\_473B10+75r