Vmp hash init analysis

Form addr of 409113

vR12 = MapViewOfFile() self

M1 = vNand4(vR12,vR12) ; EFLAG 处理

vR15 = Flag of vNand4(M1,M1)

vR8 = vNand4(M1,M1)

M2 = vNand4(FFFFFFBF,vR15) ; FLAG 判断

M3 = vShr4(M2,40)

vR12 = JAdr = vAdd4(M3,BaseAddr)

M4 = vAdd4(vR9,C67121D3) ; vR9 = 0033F698

jmp

vR8 = vAdd4(M4,398ECE2D)

; vR0 = MapViewOfFile() self

vR15 = 0033FE98

M4 = vAdd4(8,vR15)

vWriteMemSs4(M4,vR0)

; vR4 = 0

vR11 = vR9 = vAdd4(40C7A3,vR4)

vR6 = 4 ; 循环次数

; vR8 = 0033F698 vR1 = AEE9A100

M5 = vAdd4(vR8,C67131D3)

vR12 = 0

vR14 = vAdd4(M5,398ECE2D)

vR8 = AEE9A100

vR13 = 0040C7A3

vR11 = 0033FE98

vR3 = 4

vR15 = [vR13]

vR10 = bswap(vR15)

M6 = vNand4(vR10,vR10)

M7 = vNand4(M6,D7B70668) ; = 2848B890

M8 = vNand4(2848F997,vR10)

vR6 = vNand4(M8,M7)

vR15 = vShrd(vR6,vR6,14)

M9 = vNand4(vR15,vR15)

M10 = vAdd4(M9,247676BB)

vR10 = vNand4(M10,M10)

M11 = vNand4(vR10,vR10)

vR2 = Flag of vAdd4(M11,FFFFFFFF)

M12 = vAdd4(M11,FFFFFFFF)

vR6 = Flag of vNand4(M12,M12)

M13 = vNand4(vR2,vR2)

M14 = vNand4(M13,FFFFF7EA) ; = 00000011

M15 = vNand4(vR6,vR6)

M16 = vNand4(M14,815)

vR0 = vAdd4(M16,M14)

M17 = vNand4(vR0,FFFFFFBF) ; 标志位

M18 = vShr4(M17,4)

vR4 = JAdr = vAdd4(BaseAddr,M18) ; jmp switch

vR2 = vR4

; vR2 = 344B65ED

M19 = vNand4(vR2,vR2)

M20 = vNand4(M19,0CBF401F6) ; = 340B6409

M21 = vNand4(vR2,340BFE09)

vR15 = vNand4(M20,M21) ; JAdr

; vR14 = 0033F698

M23 = vAdd4(vR14, 0C67131D3)