Subject: [CODE] 4.0 server damage hook
Posted by iRANian on Sat, 30 Jun 2012 19:38:38 GMT
View Forum Message <> Reply to Message

This hooks the start of 4.0's DefenseObjectClass::Apply_Damage() hook, executes its code and then jumps 8 byte down 4.0's hook (so the 4.0 code is executed like normally). All damage done should pass through this hook but I'm not sure. I didn't include the definition of some of the hooking functions I use because I'm lazy. Took me a bit to find an Apply_Damage() function that hit my breakpoint..

```
int Calculate_Address_From_Displacement(int JMPStartAddress)
{
 char OpCodes[5];
 int Displacement, Address;

 Hooking::ReadMemory(JMPStartAddress, OpCodes, 5); // 0x004B4910 is where the JMP opcode (E9) starts, next 4 are the displacement/relative address

 memcpy(&Displacement, OpCodes+1, sizeof(char)*4); // OpCodeBuffer+1 or we'll also read the JMP opcode

 Address = JMPStartAddress + 5 + Displacement;
 return Address;
}

Hook *ApplyDamageHook = new Hook;
int TTApplyDamageAddress = 0;
int TTApplyDamageJMPAddress = 0;

bool _cdecl Apply_Damage_Hook(DefenseObjectClass *Defense, OffenseObjectClass *Offense, float DamageMultiplier, int Unk1)
{
 Console_Output("Warhead = %d\n",Offense->Get_Warhead());
 Console_Output("Unk1 = %d\n", Unk1);
 Console_Output("Health = %f\n", Defense->Get_Health());
 Console_Output("Damage = %f\n", Offense->Get_Damage());
 Console_Output("Multiplier = %f\n", DamageMultiplier);
 Console_Output("Damager = %s, Victim = %s\n",
Commands->Get_Preset_Name(Offense->Get_Owner()),
Commands->Get_Preset_Name(Defense->Get_Owner()));

 return true;
}

void _declspec(naked) ApplyDamageHook_Glue()
{
 _asm
```

```
 {
  push ebp
  mov ebp, esp
  push ecx // save ecx
  push [ebp+0x10]
  push [ebp+0xC]
  push [ebp+8]
  push ecx
  call Apply_Damage_Hook
  add esp, 16

  pop ecx // restore ecx

  test al, al
  jz NoDamage

  pop ebp
  mov al, 1
  mov edi, TTApplyDamageJMPAddress
  jmp edi

NoDamage:
  pop ebp
  retn 0ch
 }
}

/* in your installation function add: */

 TTApplyDamageAddress = Calculate_Address_From_Displacement(0x00689780); // Hook from
DefenseObjectClass::Apply_Damage
 TTApplyDamageJMPAddress = TTApplyDamageAddress + 8;
 Console_Output("TT Apply Damage address = 0x%X\n", TTApplyDamageAddress);
 ApplyDamageHook->Install('\xE9', TTApplyDamageAddress, (int)&ApplyDamageHook_Glue, "");
// jump hook

/* end installation function */
```
