Exemples en WLangage (issus du site de l'éditeur)

Classe WinDev anti Debugging

par Emmanuel Lecoester

Date de publication : 23 Mai 2010

Dernière mise à jour : 23/05/2010

Ensemble d'exemples WinDev pertmettant de vérifier la coloration syntaxique

0 - Fonction « IsDebuggerPresent »

0-A - Concept

0-B - Code

```
PROCEDURE Protect_IsDebuggerPresent(type)
SELON type
 CAS 1
  RENVOYER API ("KERNEL32","IsDebuggerPresent")
 CAS 2
  hMod est un entier = API ("KERNEL32","GetModuleHandleA","KERNEL32.dll")
  Adr est un entier = API ("KERNEL32","GetProcAddress",hMod,"IsDebuggerPresent")
  ByteRead est un entier sans signe sur 1 octets
  Transfert (&ByteRead,Adr,1)
  SI (ByteRead)<>0x64 ALORS
   RENVOYER Vrai
  SINON
   RENVOYER Faux
  FIN
 CAS 3
  AdrPEB est un entier sans signe sur 4 octets = :GET_Adresse_PEB ()
  adrRet est un entier sans signe sur 1 octet = 0x0
  Transfert (&adrRet,AdrPEB+0x2,1)
  RENVOYER adrRet
 AUTRE CAS
FIN
```

I - Fonction « Find Window »

I-A - Concept

I-B - Code

```
PROCEDURE Protect_FindWindow()
OllyFindWindow est une chaîne = "OLLYDBG"
RENVOYER API ("USER32.DLL","FindWindowA",OllyFindWindow,0)
```

II - « NTGlobalFlag »

II-A - Concept

II-B - Code

```
PROCEDURE Protect_NTGlobalFlag()
PEB est un entier sans signe sur 4 octets = :GET_Adresse_PEB ()
AdrTmp  est un entier sans signe sur 1 octet = 0x0
PEB = PEB+0x68
Transfert (&AdrTmp,PEB,4)
SI AdrTmp = 0x70 ALORS
 RENVOYER Vrai
SINON
 RENVOYER Faux
FIN
```

III - « ProcessHeap »

III-A - Concept

III-B - Code

```
PROCEDURE Protect_ProcessHeap()

AdrTmp  est un entier sans signe sur 4 octet = 0x00000000
AdrTmp2  est un entier sans signe sur 1 octet = 0x00
PEBest un entier sans signe sur 4 octets = :GET_Adresse_PEB ()
AdrTmp = (PEB+0x18)
Transfert (&AdrTmp,AdrTmp,4)
Transfert (&AdrTmp2,AdrTmp+0x10,1)
SI AdrTmp2<>0x0 ALORS
 RENVOYER Vrai
SINON
 RENVOYER Faux
FIN
```

IV - « CheckRemoteDebuggerPresent »

IV-A - Concept

IV-B - Code

```
PROCEDURE Protect_CheckRemoteDebuggerPresent()
SI SysVersionWindows(sysVersionPlateForme)="NT" ALORS
 hMod est un entier = API ("KERNEL32","GetModuleHandleA","KERNEL32.dll")
 adrCRDP est un entier sans signe sur 4 octets = API
 ("KERNEL32","GetProcAddress",hMod,"CheckRemoteDebuggerPresent")
 val_param est un tableau fixe de 2 entiers sur 4 octets
 val_param[1] = -1
 val_param[1] = 0x0
 :Emulate_Call_Function (adrCRDP,val_param)
 RENVOYER 0
SINON
 RENVOYER 0
FIN
```

V - « Registry OllyDbg Detected »

V-A - Concept

V-B - Code

```
PROCEDURE Protect_Registry(type)
SELON type
 CAS 1
  SI RegistreLit ("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\AeDebug","Debugger")<> "" ALORS
   RENVOYER Vrai
  SINON
   RENVOYER Faux
  FIN
 CAS 2
  SI RegistreExiste( "HKEY_CLASSES_ROOT\exefile\shell\Open with Olly&Dbg\command") ALORS
   RENVOYER Vrai
  SINON
```

```
    RENVOYER Faux
   FIN
  CAS 3
   SI RegistreExiste( "HKEY_CLASSES_ROOT\dllfile\shell\Open with Olly&Dbg\command") ALORS
    RENVOYER Vrai
   SINON
    RENVOYER Faux
   FIN
  AUTRE CAS
FIN
```

VI - « OutputDebugString »

VI-A - Concept

VI-B - Code

```
PROCEDURE Protect_OutputDebugString()
QUAND EXCEPTION DANS API ("KERNEL32","OutputDebugStringA","%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s")
 RENVOYER Faux
FAIRE
 RENVOYER Vrai
FIN
```

VII - Complément :

VII-A - Fonction GET_Adresse_PEB

```
PROCEDURE PRIVÉE GET_Adresse_PEB()
AdrTEB est un entier = :Get_Adresse_TEB ()
AdrPEB est un entier sans signe sur 4 octets
Transfert (&AdrPEB,AdrTEB+0x30,4)
RENVOYER AdrPEB
```

VII-B - Fonction GET_Adresse_TEB

```
PROCEDURE PRIVÉE Get_Adresse_TEB()
RENVOYER API ("NTDLL.DLL","NtCurrentTeb")
```