

**Menu**[News](#)[Forum](#)[Liens](#)[Outils](#)[Livre d'or](#)**Tutoriaux**[Flash Decompiler](#)[Cracking](#)[Photoshop](#)

Cracking : le .net, incrackable ?!

Land-Of-Bork0

Salut à tous ! 😊

Dans ce tuto, on va s'attaquer a une protection réputée pour etre incrackable...le .net (dotNet).

🤔 Euh, le .net c'est une extension de site web ?! 😊 Et puis pourquoi dotnet, .net ?

Le dotnet (dot veut dire point '.' in english) est la nouvelle génération d'application multiplateforme microsoft 😊 Simple non.. Bon ok, je refais 😊 Je vais pas vous faire un cours détaillé sur le .net et le frameworks, on va s'intéresser à la partie langages de programmation. Vous devez surement connaître (au moins de nom) les langages de programmation basiques comme le C, C++, Visual Basic, Delphi, Java, PHP, ASP ? Et bien, microsoft a développé des nouveaux langages de programmation tel le C#.net (prononcez Csharp, sharp = #), le C++.net, le Visual Basic.net, l'ASP.net, le Delphi.net, etc... qui fonctionne à condition d'avoir installer ce qu'on appelle le FrameWorks, c'est une 'plate-forme' qui permet de faire fonctionner toutes les applications programmées dans n'importe quel langage .net, vous pouvez telecharger la dernière version du frameworks sur le site de microsoft. Pour faire des applications dans les langages .net (à noter que le langage .net le plus utilisé par microsoft est le C#) vous devez disposer soit de microsoft visual studio 2005 (ou 2003) mais vous pouvez aussi prendre les versions express (gratuites) qui permettent de programmer dans un seul langage et sont un peu limités (enfin, limité, vous avez quand meme énormément de possibilités encore !). N'oubliez pas de telecharger le frameworks !

Je vous ai concocté un petit crackme en C#.net 😊

[Telecharger le crackme](#) (140 Ko)

On le lance, il nous demande un joli password, on en met un bidon et hop :



Vous pouvez le scanner avec PEid, il vous dira "Microsoft Visual C# / Basic .NET"

Bon, on va d'abord tester avec Olly 😊 Lancez le, après un long moment d'attente, on voit du code apparaitre, allez voir dans les SDR :

```

ADD     ERX,384500
PUSH    EAX,00000000
IMUL    ESI,DWORD PTR SS:[EBP+ECX*2+65],79
IMUL    ESI,DWORD PTR SS:[EBP+ECX*2+65],79
MOV     DWORD PTR DS:[EAX+A8],EDX
ADD     EAX,10006
MOV     DWORD PTR DS:[ECX],ntdll.7C92030C
PUSH    ntdll.7C923774
PUSH    ntdll.7C92370C
PUSH    ntdll.7C924B12
PUSH    ntdll.7C924F1E
MOV     EBX,ntdll.7C98CE28
MOV     ESI,ntdll.7C98D040
MOV     DWORD PTR SS:[EBP-38],ntdll.7C926C5
MOV     DWORD PTR SS:[EBP-38],ntdll.7C92745
MOV     DWORD PTR SS:[EBP-2C],ntdll.7C92A18
MOV     DWORD PTR SS:[EBP-2C],ntdll.7C92AFF
PUSH    ntdll.7C92D232
PUSH    ntdll.7C92D304
PUSH    ntdll.7C92D4B0
PUSH    ntdll.7C92D594
PUSH    ntdll.7C92D53C
PUSH    ntdll.7C92D5A4
PUSH    ntdll.7C92E066
PUSH    ntdll.7C92F2BE
PUSH    ntdll.7C92F2FE
PUSH    ntdll.7C92F840
MOV     ESI,ntdll.7C92F830
PUSH    ntdll.7C92F8F6
PUSH    ntdll.7C92F93E
PUSH    ntdll.7C930BEE
CMP     EBX,ntdll.7C92030C
CMP     DWORD PTR SS:[EBP+10],10000
PUSH    ntdll.7C930D88
PUSH    ntdll.7C930D00

```

UNICODE "b:\update\update.exe"  
 ASCII "Set\_ChoiceArrayName"  
 ASCII "KU"  
 ASCII "KU"  
 (Initial CPU selection)  
 UNICODE "=:\  
 ASCII "Actx "  
 ASCII "RtlLockHeap"  
 ASCII "RtlUnLockHeap"  
 UNICODE "S-I-"  
 UNICODE "\REGISTRY\USER\  
 UNICODE "Kernel32.dll"  
 UNICODE ".dll"  
 ASCII "Refcount"  
 ASCII "Decrecount"  
 ASCII "Refcount"  
 ASCII "Decrecount"  
 UNICODE "\Registry\Machine\Software\Microsoft\Windo  
 ASCII "seeserv.dll"  
 UNICODE "CheckAppHelp"  
 ASCII ".aspack"  
 ASCII ".pcle"  
 ASCII ".force"  
 ASCII "LDR"  
 ASCII "SXS: Assembly storage resolution trying %Id  
 ASCII "SXS: Storage resolution for root number %lu  
 ASCII "SXS: Getting assembly storage root #%lu"  
 UNICODE ".Local\  
 ASCII "SXS: Assembly storage map probing root %w2 f  
 ASCII "SXS: Found good storage root for %w2 at inde  
 ASCII "SXS: RtlCreateActivationContext() called wit  
 ASCII "Actx "  
 UNICODE "=:=:\  
 ASCII "SXS: Activation context data at %p has inval  
 ASCII "SXS: Activation context data at %p has inval

Si vous etes suicidaire, vous pouvez tout regarder ligne par ligne en espérant trouver une information que vous ne trouverez pas... Pour les autres, fermez Olly, il ne sera pas de la partie aujourd'hui !

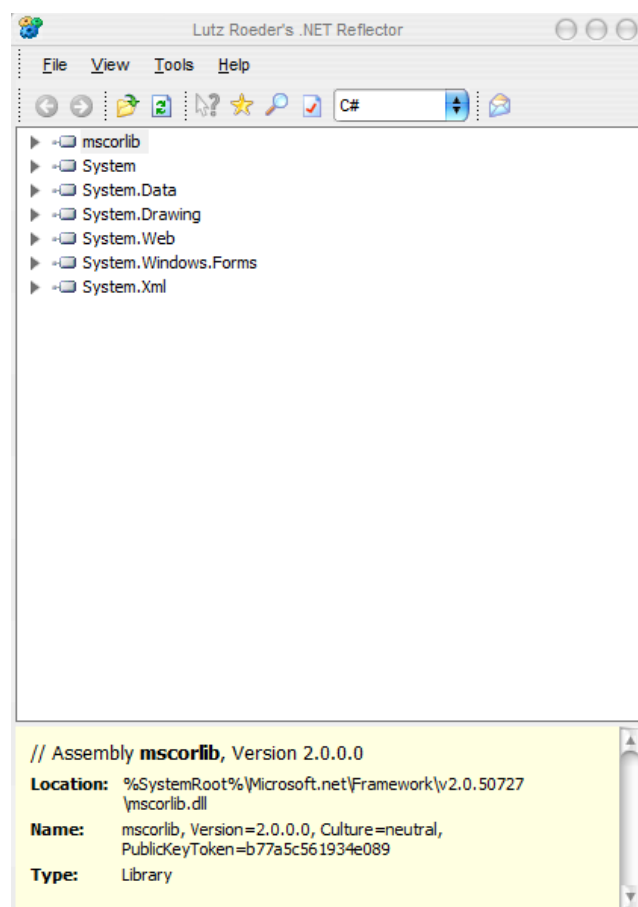


Et on fait quoi alors ?!

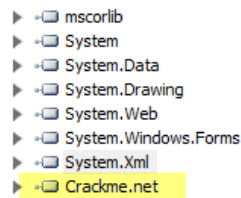
Le frameworks ayant un compilateur spécial (le meme pour tout les languages donc exactement la meme vitesse), il est possible de voir le code, après compilation, presque intact ! Il existe plusieurs logs, j'ai choisi "reflector qui est simple et petit...

[Telecharger reflector](#)

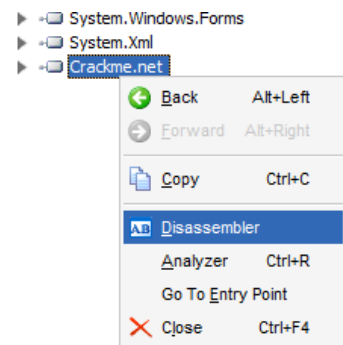
Après l'avoir extrait n'importe ou, lancez le :



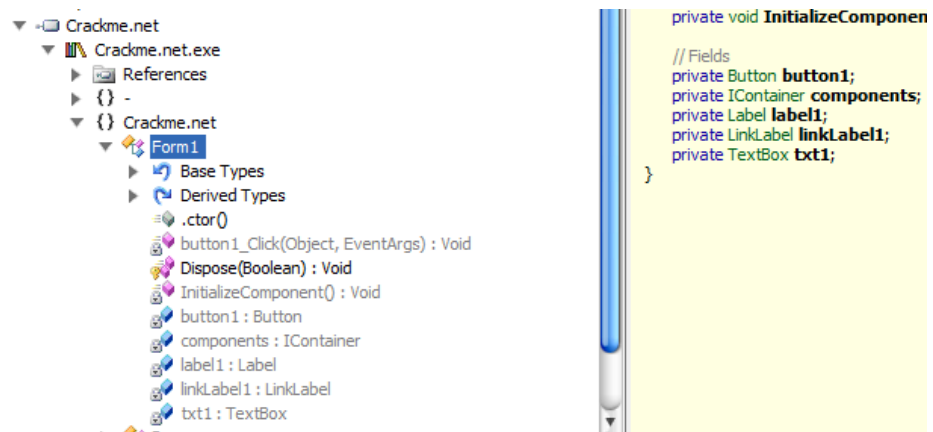
ne nous occupons pas du coeur, mais regardons les menu, on voit "File", soyons fou, essayons d'ouvrir notre petit crackme ! (File » Open » crackme.exe)



Crackme.net est apparu dans le cœur ! Cliquez dessus, le petit menu du bas change, mais rien de bien intéressant... Faites clic droit » Disassembler :



Un écran s'ouvre à droite. Faites un double clic sur Crackme.net dans le panneau de gauche puis cliquez sur crackme.net.exe, recliquez sur crackme.net et enfin cliquez sur form1 :



Alors, qu'est ce que c'est que tout ce charabia, pour ceu qui connaissent la programmation orientée objet ça devrait être bien plus facile :

- Form1 = C'est la fenêtre principale du programme
- button1 = le bouton "valider !"
- label1 = le texte "password"
- linkLabel = le lien vers mon site
- textBox (txt1) = la "boîte à texte" où on rentre le password

On se retrouve avec tout les éléments de la form dans le menu de droite et dans le panneau de gauche on retrouve les mêmes avec quelques autres trucs en plus

On va s'intéresser à button1\_click, qu'est ce que c'est ?! Ce sont les événements lorsqu'on clique sur le bouton "valider", notre routine va être sûrement ici ! Cliquez dessus :

```
private void button1_Click(object sender, EventArgs e)
{
    if (this.txt1.Text == "modem")
    {
        MessageBox.Show("Identification Reussie...", "Bon Pass", MessageBoxButtons.OK, MessageBoxIcon.Asterisk);
    }
    else
    {
        MessageBox.Show("Mauvais identifiants...", "Et non !", MessageBoxButtons.OK, MessageBoxIcon.Hand);
    }
}
```

Ceux qui font de la progz auront déjà compris, pour les autres, une petite explication :

`private void button1_Click(...)` = indique le début des événements d'un clic sur le bouton

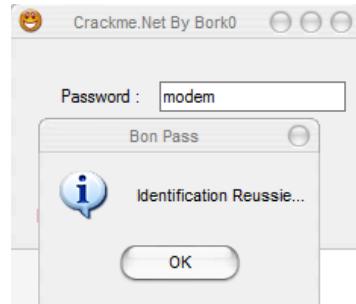
`if(this.txt1.Text == "modem")` = Littéralement "Si le texte de la boîte de texte txt1 est égal au mot modem alors", c'est une condition !

`MessageBox.Show("identification réussie",...)` = Affiche une message box (boîte de message contenant le message identification réussie ! C'est le bon message.

`else` = Sinon (si txt1.text n'est pas égal a modem alors)

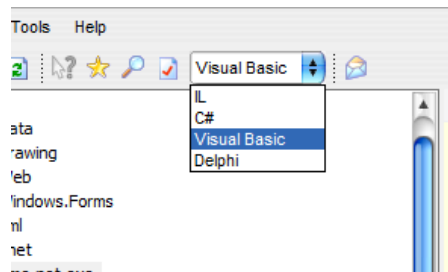
`MessageBox("mauvais identifiants", ...)` = Affiche la message box d'erreur !

Vous pouvez tester de mettre "modem" et hop :



Pour les autres crackmes en .net, c'est toujours le même système ! Ici, ce n'est pas vos talents de crackers qui seront mis à l'épreuve mais plutôt votre bonne analyse du code et une bonne connaissance des langages de programmation

Maintenant, je vais vous montrer comment changer le langage de programmation affiché, imaginons que vous soyez une brêle en C# mais que vous soyez super fort en delphi ou vb, on peut changer le langage ! Pour cela, faites comme sur l'image :



Et hop, le langage change instantanément ! Pratique non ?

Vous l'aurez sûrement remarqué, on ne peut pas "cracker" à proprement dit, à savoir modifier les sauts conditionnels et tout le troupin habituel quoi, ben oui, c'est l'inconvénient, vous ne pourrez pas le cracker mais vous pourrez avoir la source et donc retrouver intégralement les routines de génération du sérial, les password !

je n'ai encore jamais testé cette technique sur des programmes payants, mais à moins qu'il existe une sécurité particulière, ça doit sûrement marcher aussi 😊

Enjoy 🍷

[Keygenner un keymaker](#) / [Analyser le code d'un crackme](#)

[RETOUR EN HAUT](#) / [INDEX DU CRACKING](#) / [INDEX DU SITE](#) / [FORUM](#)

