

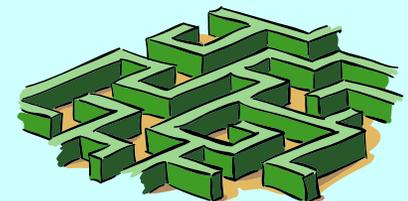


***La rétroconception,
quel intérêt pour le RSSI ?***

Bruno Kerouanton, CISSP

<http://bruno.kerouanton.net>

Rump Session
SSTIC 2006 – Rennes, France



Le point de vue de « Monsieur tout le Monde »

C'est interdit !

Législation répressive

Ce n'est pas bien !

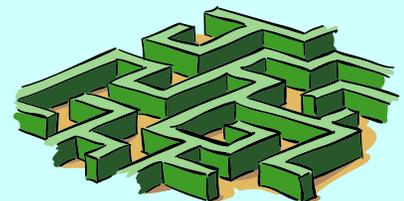
Connotation négative, « hackerish »

C'est pour les *geeks* !

Compétences pointues nécessaires

Ca ne sert à rien !

Fastidieux et sans garantie de résultat



Le point de vue du professionnel de la sécurité

C'est interdit !

Tout dépend de ce que l'on (en) fait

Ce n'est pas bien !

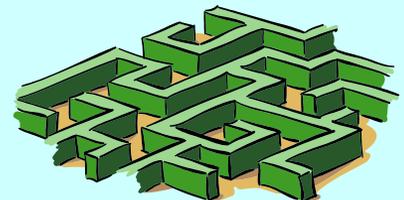
Usage professionnel et éthique possible

C'est pour les *geeks* !

Outils de plus en plus performants / intuitifs

Ca ne sert à rien !

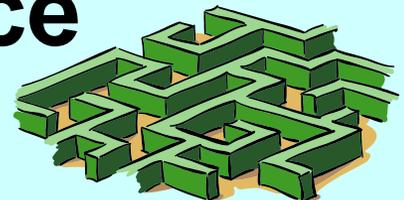
De nombreux usages utiles et légaux



Quelques applications pour le RSSI :

- Écarter les produits mal finalisés et “suspects”
- Évaluer la maintenabilité
- Améliorer la gestion du parc logiciel
- Évaluer rapidement les produits cryptographiques
- Effectuer des audits “live” de plateformes

➔ Sécurité accrue, contrôle renforcé



1. Écarter les produits mal finalisés

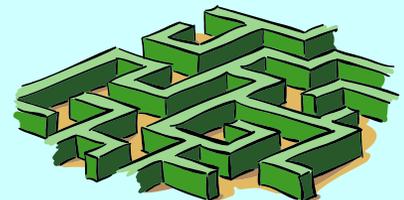
Exemple : Nombreuses références au code source dans la version finale :

```
push    offset asc_6FDC34; "C:/ob/bora-19175/bora/lib/vndbschema/vm" ...  
mov     [esi+908h], eax  
call   sub_553B80  
mov     eax, [esi+90Ch]
```

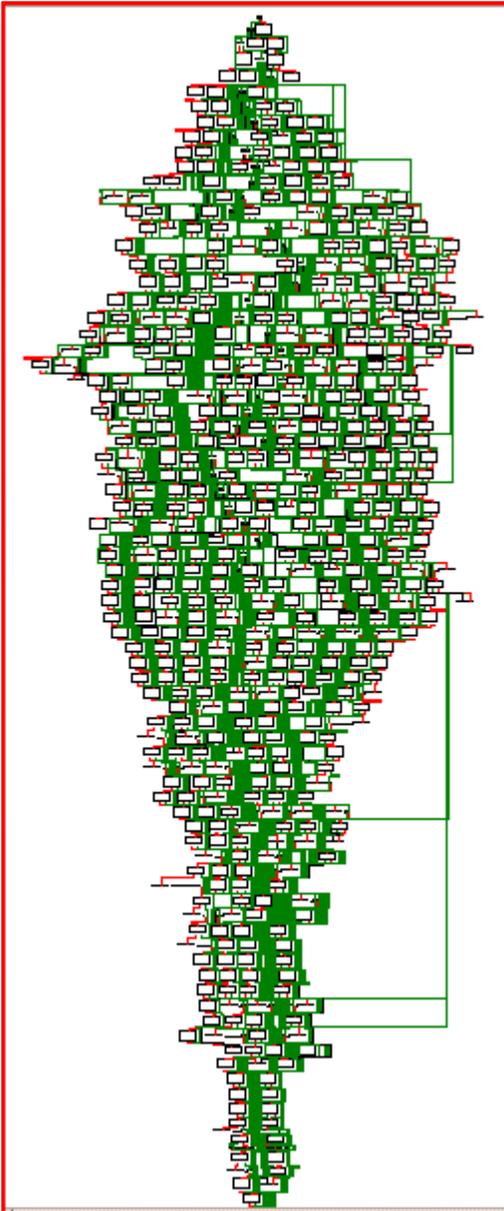
constat : versions de débogage livrées / vendues

- Contrôle qualité au rendez-vous ?
- Pression commerciale ?
- Logiciel fourni plus lent voire instable ?

→ **Permet une sélection pertinente des produits et solutions**



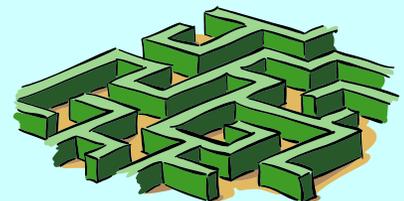
2. Évaluer la maintenabilité



Exemple :
fonctions « fourre-tout ».



**Quid de la pérennité,
de la maintenabilité ?**

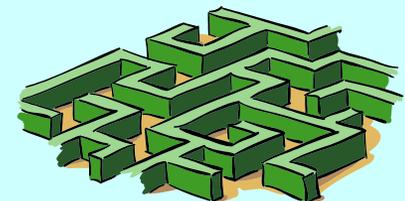
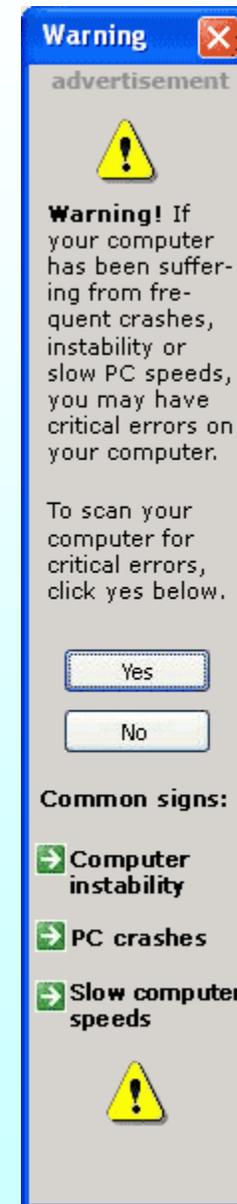


3. Écarter les produits “suspects”

➤ Spywares, backdoors, etc.

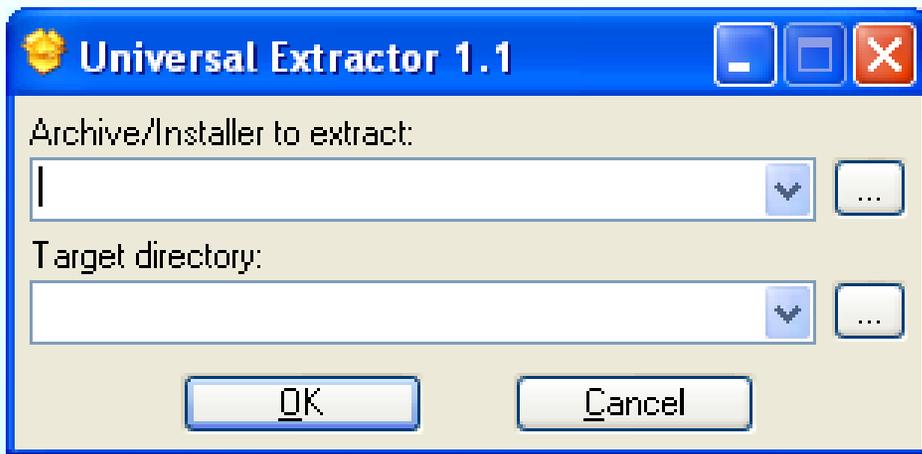


➔ Renforce la sécurité

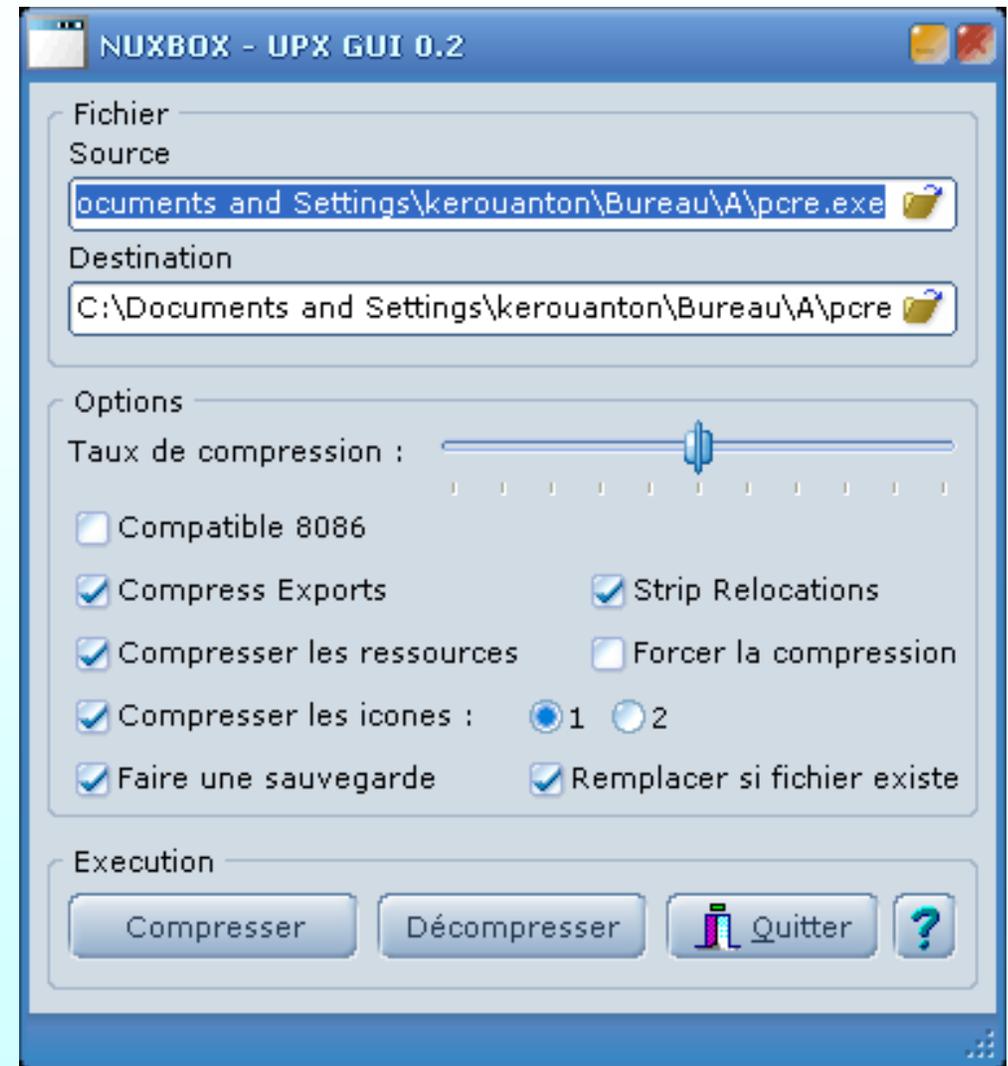


4. Mieux gérer le parc logiciel

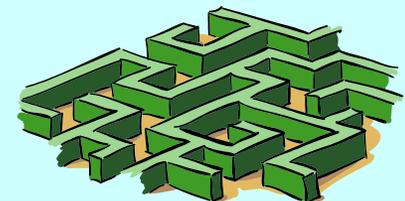
→ Repackaging / reparamétrage des applications.



→ Optimisation des installations et de la taille des exécutables.



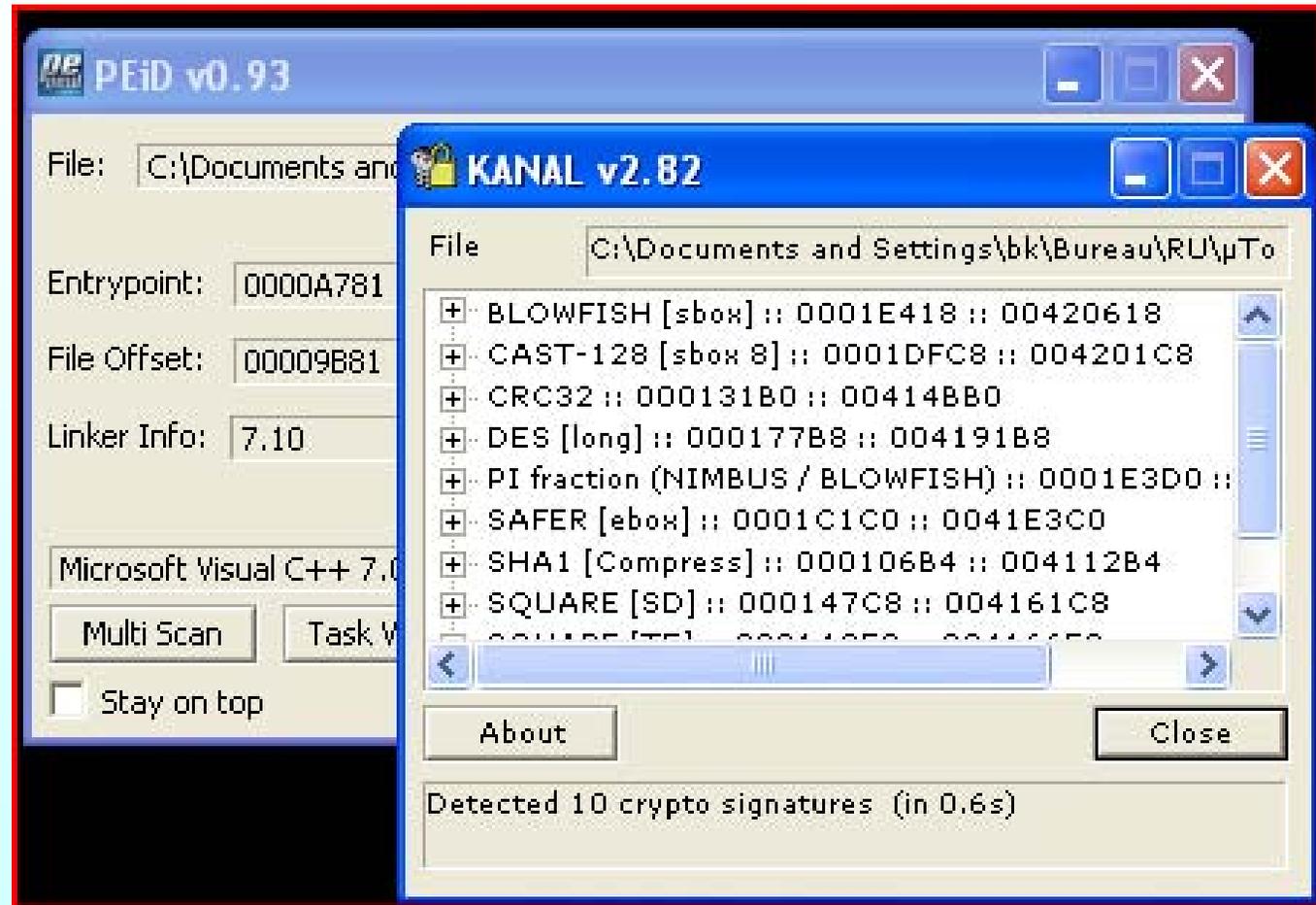
→ **Bénéfice** - pour les administrateurs
- pour le RSSI



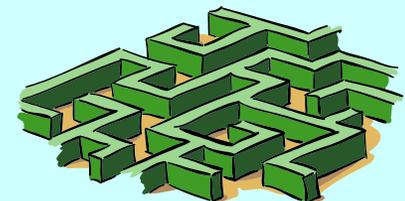
5. Evaluer rapidement les produits cryptographiques

Algorithmes annoncés réellement implantés ?

→ moins de mauvaises surprises !



...face aux produits "Snake-Oil"



6. Effectuer des audits « live »

- ➔ Surveillance de processus douteux, gestion de parc.

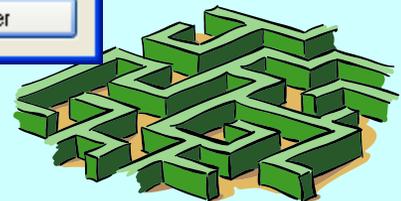
The screenshot displays a live audit environment. In the foreground, a dialog box titled "Compressed code?" asks: "Quick statistical test of module 'enigma' reports that its code section is either compressed, encrypted, or contains large amount of embedded data. Results of code analysis can be very unreliable or simply wrong. Do you want to continue analysis?" with "Oui" and "Non" buttons.

Behind the dialog, OllyDbg shows assembly code for the CPU main thread of clamwin-0.88.2.3-setup.exe. The assembly includes instructions like PUSH EBP, MOV EBP, ESP, ADD ESP, -2C, PUSH EBX, PUSH ESI, PUSH EDI, XOR EAX, EAX, and MOV DWORD PTR SS:[EBP-10], EAX.

Process Explorer in the background shows a list of processes with columns for Process, PID, CPU, and De. The process clamwin-0.88.2.3-setup.exe is highlighted with a PID of 3888.

On the left, a file properties window shows details for a file in C:\Documents and Settings, including file size, CRC-32, MD5, and a list of sections (.text, .rdata, .data, .rsrc).

At the bottom, a memory dump window shows the hex dump and ASCII representation of memory starting at address 0040A000. The ASCII column shows the text ".!@.E@.@.\!@.S@", "2!!i'Runtime ex", and "r at 00000", followed by "0.Error.". The status bar at the bottom indicates "Analysing clamwin: 234 heuristical procedures, 149 calls to known, 37 calls to guessed function" and is in a "Paused" state.



7. Veille : apprendre l'état de l'art...

➤ Lecture de tutoriaux, de blogs, de forums...

Hex Blog
About IDA Pro, decompilation, programming,
binary program analysis, information security.
By Ilfak Guilfanov

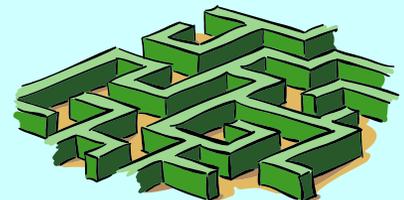
BeatriX

SECURITECH

OpenRCE.org

COMPRENDRE
LE
Kaine #5

➔ Se tenir informé pour ne pas dire “je ne savais pas” !!



... parfois même en s'amusant !

➔ Via les sites "underground" ...

SO... A QUOI IL LOOKED LIKE TON FRIEND?
PFFIOU! ON A FAIT VITE

BEN EN FAIT QUAND ON MATTE UN PEU MA ROUTINE INTERNE, IL RESSEMBLE UN PEU A CA...

LISTING IDA

```
.text:00401883 lea    eax, [ebp+buffer_nom]
.text:00401886 push   eax
.text:00401887 push   offset aS      ; "%s"
.text:0040188C call   scanf
```

RECUPERATION DE LA LONGUEUR DU NOM DANS EAX

```
.text:004018A7 lea    eax, [ebp+buffer_nom]
.text:004018AA push   eax
.text:004018AB call   strlen
.text:004018B0 add    esp, 10h
.text:004018B3 mov    eax, eax
.text:004018B5 cmp    eax, 5
.text:004018B8 ja     short _01
.text:004018BA add    esp, 0FFFFFFF4h
.text:004018BD push   offset aStringXsTropPe ; "String XS ! Trop petit : name > 5 !\n\n"
.text:004018C2 call   printf
```

PRISE DU NOM. STOCKAGE EN [BUFFER_NOM]

SI C'EST INFÉRIEUR A 6, C'EST MORT

Outils in-dis-pen-sables !

Collections d'outils de Mark Russinovich (sysinternals.com)
et de Nir Sofer (nirsoft.net)

PeID (+ plugins : Krypto Analyzer etc.)

Très pratique et simple d'utilisation.

Universal Unpacker

Décompresse TOUT... ou presque.

OllyDbg (+ plugins)

« LE » débogueur par excellence... et gratuit en plus.

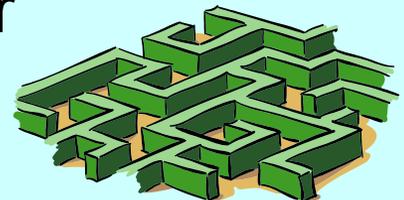
DataRescue IDA Pro (+ plugins)

Achetez-le, vous ne le regretterez pas. Franchement !

Vmware Workstation ou Microsoft Virtual Server

Ne prenez pas de risques en travaillant.

... et bien d'autres encore...



0 €

€€€