26/01/2020

Veille Technologique

Sécurité informatique

Pierre Duveau
INSTITUTION DES CHARTREUX – LYON CROIX-ROUSSE

Table des matières

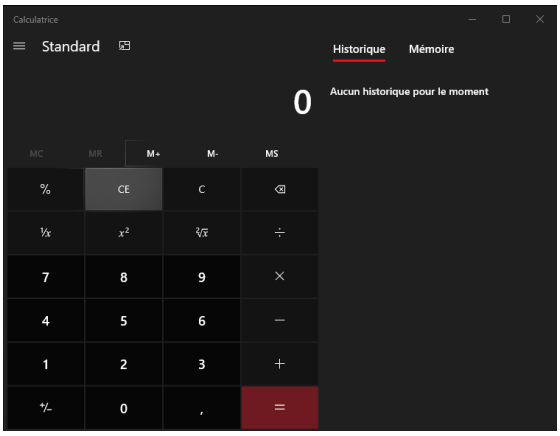
Dans le cadre de la deuxième année du BTS SIO, j'ai été amené à rédiger une veille technologique sur un type de sécurité informatique, c'est-à-dire choisir un sujet de veille, faire des recherches et enfin de compte le développer.

I. Qu'est-ce que le reverse engineering ?

Le reverse engineering (rétro-ingénierie) aussi appelé 'reverse' (inverse) dans le jargon informatique c'est le fait de comprendre le fonctionnement d'une application ou d'un système et d'être capable d'en recréer un à l'identique.

Pour ça il y a plusieurs possibilités :

1. L'analyse des fonctionnalités d'un point de vue extérieur :



On repère plusieurs fonctionnalités :

- L'ajout de chiffres
- La possibilité d'effectuer des / L'exécutions d'opérations simples ou complexes
- Un historique des calculs.
- La possibilité de peut passer la calculatrice en mode minimaliste, la fermer, la mettre en pleine écran ou la minimiser.

Figure 1Calculatrice de Windows 10

A travers ces exemple, il peut paraitre facile de recréer un programme simple, d'un point de vue logique. Cependant certains programmes nécessitent de vrais experts afin de pouvoir recréer certaines fonctionnalités.

2. L'utilisation d'un programme de décompilation.

C'est un programme qui va décompiler un type d'application afin de pouvoir directement visionner le code source.

Il existe de nombreux programme pouvant décompiler des .exe, les plus connus sont :

- ILSpy
- IDA Pro
- X64dbg
- Etc…

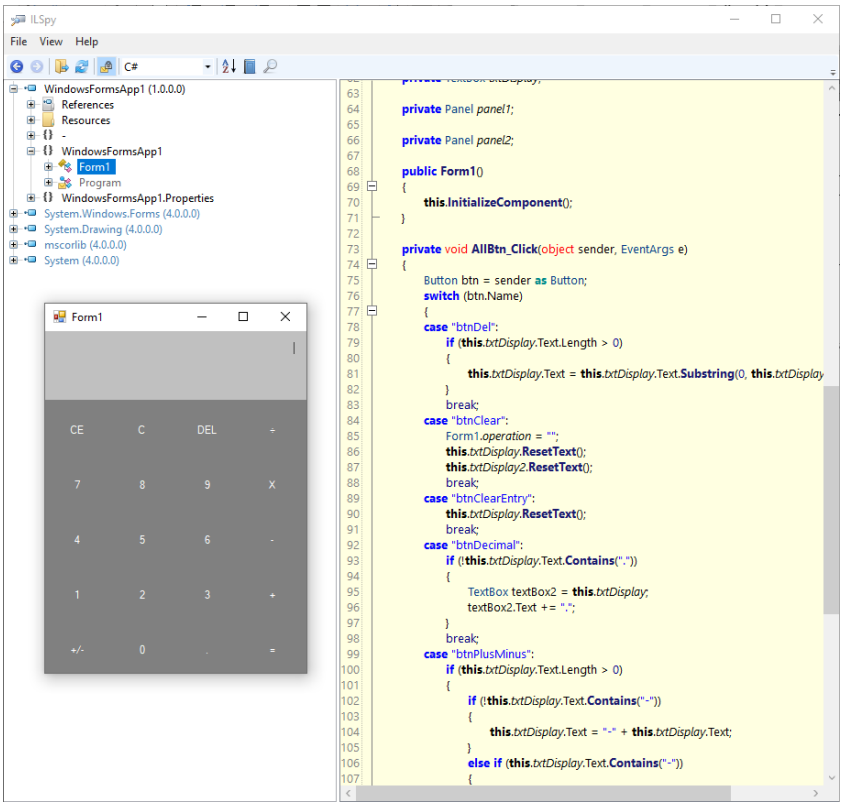


Figure 2 Application similaire décompilé avec ILSpy

II. Les risques du reverse engineering :

Les risques du reverse engineering sont nombreux, si les programmes ne sont pas protégés, il deviendra alors facile de récupérer les données de certaines applications, et permettre ainsi possiblement à des entreprises concurrentes de récupérer les données.

Cependant il existe plusieurs outils qui peuvent permettre de protéger ces applications, tels que .NET Reactor ou encore ConfuserEx. Leur but est d'empêcher des outils comme IDA, ou ILSpy de fonctionner en bloquant leur fonctionnement ou en rendant le code inintelligible.

Figure 3 Image après avoir été protégée par .Net Reactor

III. Conclusion :

Le reverse engineering est une technique peu connue du grand publique, elle est souvent utilisée dans le monde professionnel, servant pour la plupart à recréer les fonctionnalités du concurrent comme par exemple le système de like de Facebook et celui de LinkedIn qui sont très similaire.

Cependant cela relève de nombreuses questions, notamment dans le domaine du droit d'auteur par exemple ou quant à l'originalité d'une œuvre. Quand on fait du reverser engineering il faut donc prendre en compte que l'on doit récupérer des fonctionnalités et non pas copier les fonctionnalités d'une autre solution.

Webographie :

A. Reverse Engineering :

https://connect.ed-diamond.com/MISC/MISC-092/Reverse-Engineering-ce-que-le-droit-autorise-et-interdit

https://connect.ed-diamond.com/MISC/MISCHS-007/Introduction-au-reverse-engineering

https://www.solutions-numeriques.com/dossiers/decompilation-et-analyse-de-logiciel/

https://www.apriorit.com/dev-blog/366-software-reverse-engineering-tools

https://www.apriorit.com/dev-blog/364-how-to-reverse-engineer-software-windows-in-a-right-way

B. Non au Reverse Engineering

https://www.developpez.com/actu/88734/-Vous-n-avez-pas-le-droit-d-appliquer-le-reverse-engineering-sur-notre-code-le-coup-de-gueule-de-la-directrice-de-la-securite-d-Oracle/

C. Vidéo de la calculatrice décompilé :

https://www.youtube.com/watch?v=JJge3PCdGb8