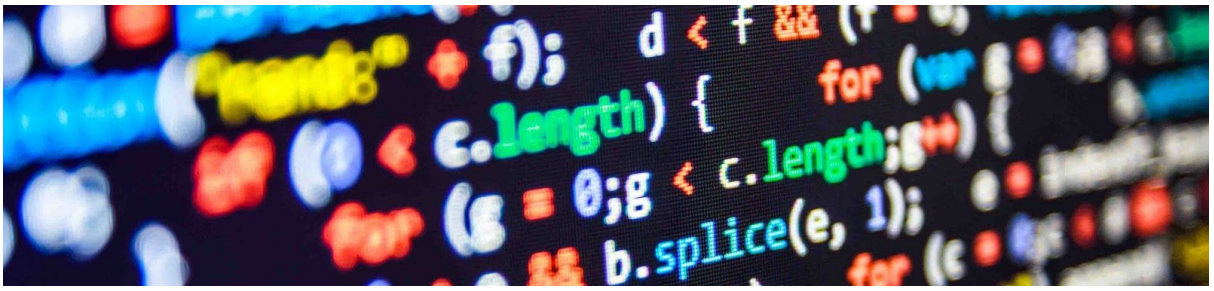
# Les limitations des anti-virus : analyse et POC




PART 2

## Introduction

Maintenant que nous connaissons suffisamment bien notre ennemie, nous pouvons commencer à contre-attaquer !

Dans cette partie, nous allons nous concentrer uniquement sur le contournement des analyses statiques, ou plus simplement : comment modifier la signature d'un payload ?

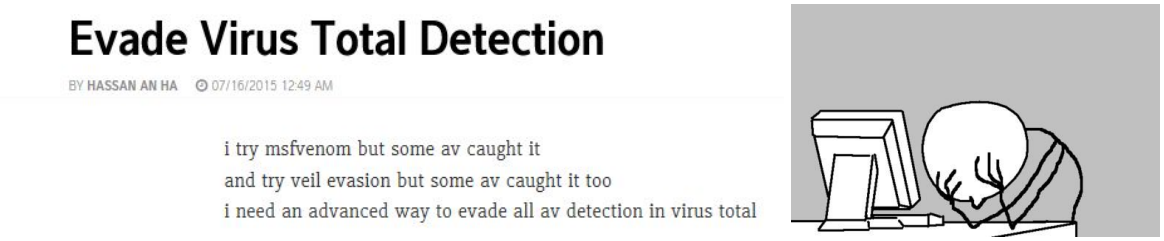
## II. Modification manuelle de signature

Avant de commencer, je dois préciser quelques points. En premier, vous avez devant les yeux une synthèse de mes recherches qui contient uniquement les principes théoriques de l'évasion d'antivirus. Le pdf complet comportant tous les détails, les commandes, les fonctions, et les descriptions de ces dernières sera présent en bas de page !

Deuxièmement, j'aborderai la phase de compilation dans une autre partie, mais les commandes qui y sont relatives ne seront volontairement pas présentes, de façon à ne pas délivrer un tutoriel clé en main !

Enfin, les scans réalisées sont effectuées avec VirusTotal. Je vous entend crier, arrêtez ! Effectivement, à force d'utiliser des outils censés nous fournir du FUD, nous avons tous été conditionnés à fuir ces scans en ligne comme la peste. C'est tout à fait vrais pour certains softs (TheFatRat, Shelter, Veil-evasion, etc ..) qui utilisent les mêmes templates pour générer leurs payloads. Soumettre à un scan en ligne un payload provenant de ce genre de soft tue littéralement le travail de l'auteur. Dans le cas présent, je me fiche de garder des

payloads FUD, étant donnée qu'il est si facile d'en créer de nouveaux, je ne vais pas me priver !




## II.I Modification manuelle de signature assembleur

Une des première façon de modifier la signature d'un payload consiste à ajouter des instruction dans le code assembleur, au milieu et tout autours de la signature.
Le principe est de ne surtout pas modifier les instructions assembleurs de bases, mais d'ajouter des lignes superficielles.
Cette méthode à de nombreuses limites, notamment le ratio entre le temps de modification et l'efficacité du résultat.

Dans un premier temps, il faudra générer un simple payload au format .binary. Ici, je n'utiliserai que des reverse_tcp via meterpreter, tant ceux-ci offrent des possibilités de post-exploitation intéressantes ( et aussi puisqu'il s'agit d'un des payloads les plus populaires, c'est encore plus drôle de réussir à le rendre incognito ). Pour isoler la partie du payload comportant la signature, il faut découper le fichier binaire en petites portions, jusqu'à isoler la signature le plus précisément possible.

### Add synthèse modiff sig asm

### Add synthèse modiff sig C

### Add synthès modiff sig Hex

Nous verrons plus tard qu'il est possible de rendre des payload 100% FUD, mais il est préférable de cibler un antivirus en particulier pour commencer. Ici, je choisirais Avast, tout

simplement parce qu'il s’agit d’un AV réputé et répandu, et puisque ma machine de test tourne dessus.