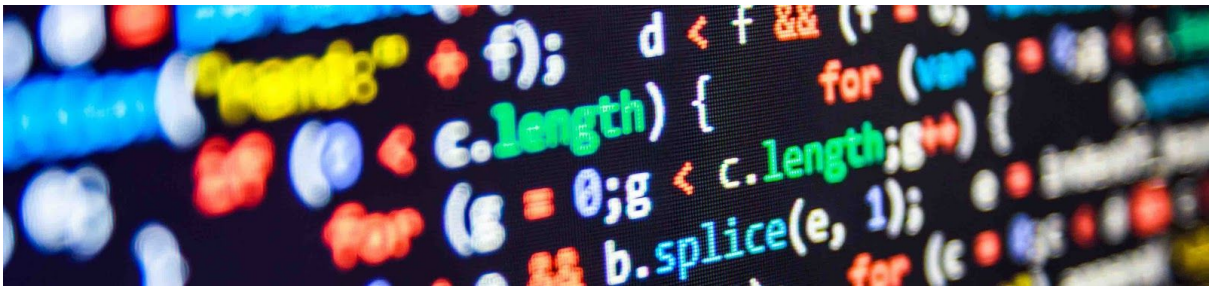
Les limitations des anti-virus : analyse et POC



PART 1

Introduction

Ah les antivirus … Une longue histoire, beaucoup de questions et d'incompréhensions.
Mais comment font ils pour nous protéger des fichiers néfastes qui trainent sur le net ? Sont-ils vraiment utiles ? Est il si facile de les contourner ?

Après plusieurs semaines de recherches et d'expérimentations sur le sujet, je pense qu'affirmer de nos antivirus qu'ils sont indispensables serait un gros mensonge, même si au final, certains semblent bien résister.

Je vous présente ici une synthèse de mes recherches, un peu plus axée sur la partie offensive, je vous l'accorde !

I. Les Outils côté Anti-Virus :

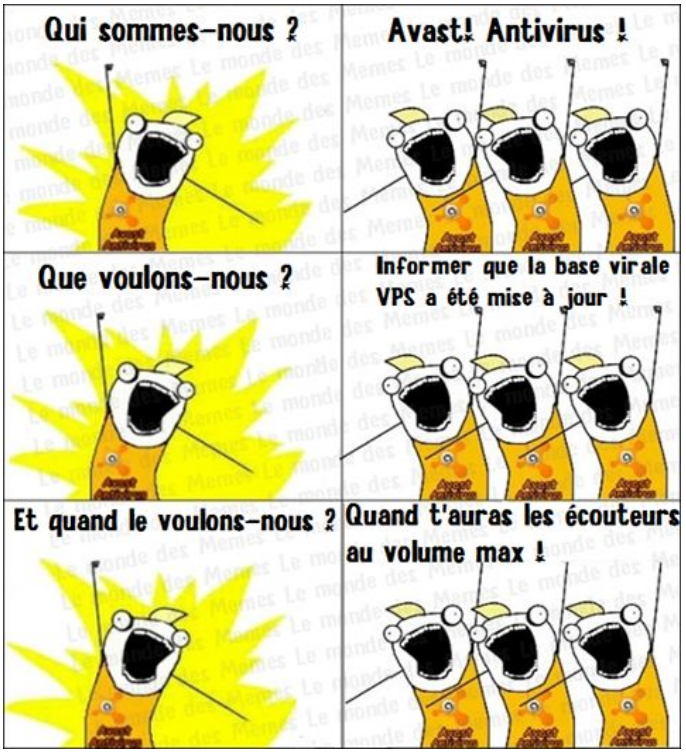
Bon, que l'on se le dise tout de même, les anti-virus disposent d'un bon gros arsenal pour détecter la plupart des payloads bêtes et méchants destinés à infecter la masse.
Pour juger des failles qu'offrent les antivirus, il faut d'abord analyser leurs méthodes de fonctionnement !

I.1. L'analyse statique (ou contrôle des signatures)

La signature d'un virus, c'est quoi ?
L'analogie est très bien trouvée et parle d'elle même : la signature d'un virus permet d'identifier de manière unique et précise un fichier étiqueté comme malicieux. Cette signature peut comprendre les premiers octets d'un fichier, des bouts de codes ou même parfois des noms de fonctions et variables génériques.
Une signature virale désigne donc une portion connue d'un fichier malveillant, présente dans certains fichiers infectés, mais pas dans les autres.
De cette façon, les compagnies d'antivirus mettent à jour d'énormes bases de données comportants des tas de signatures connues, pour bloquer les fichiers scannés en amont. Malin !

Et en plus, cette "technique" permet de couper l'herbe sous le pied à tous les petits malins qui coupleraient un virus déjà existant avec des bouts de codes à eux !

La pertinence d'un Antivirus dépend donc grandement de cette liste de signatures, et des manières employées pour la maintenir à jour. A titre d'exemple, chez presque tous les "gros" constructeurs d'AV, cette mise à jour passe notamment par un récolte d'échantillons sur nos machines, puis par une analyse en laboratoire (traitée par des machines, et dans certains cas par des humains). Cette analyse permet d'émettre un verdicte et d'étiqueter correctement un nouveau fichier.



Vous savez bien, c'est le fameux timer d'Avast qui réclame 30 minutes pour envoyer un fichier "rare" et l'analyser, avant d'enfin nous permettre de l'exécuter ! Pas pratique pour un utilisateur, mais indispensable pour les constructeurs d'AV.

Avec du recul, le principe de la reconnaissance d'un fichier via une signature peut paraître archaïque et très simple, pourtant, plus d'1/2 des entrées des bases de données d'antivirus y sont dédiées... De quoi éliminer automatiquement un tas de fichiers pas nets !

L'autre atout de cette méthode de détection réside dans le fait de pouvoir détecter des malwares avant leurs exécutions en mémoire. Ce qui est plutôt pratique.

I.2. La SandBox

Le principe est simple à comprendre, mais tout de même bluffant :
Lorsqu'un fichier est exécuté par l'utilisateur, l'antivirus le lance dans un environnement émulé pour observer le comportement de l'application, avant de la valider !
De cette façon, il est possible d'observer si une signature connue va pointer le bout de son nez après quelques secondes d'exécutions. Par signature, il s'agit ici d'une recherches de comportements pouvant altérer

Etrangement, la sandbox n'est pas très compliquée à contourner (nous y reviendrons) mais à le mérite d'être bien pensé.
Celle-ci est d'autant plus complémentaire avec la méthode de détection vue plus haut, qu'elle permet de contourner les méthodes classiques utilisées pour brouiller une signature :

le chiffrement. En y réfléchissant deux secondes, si je souhaites empêcher un antivirus de vérifier la signature de mon fichier malicieux, pourquoi ne pas juste le chiffrer, et laisser la clé de déchiffrement dans le code ?
Réponse : parce que la sandbox va lancer le fichier, déchiffrer le payload, puis se rendre compte que celui-ci correspond à une signature connue !

Complémentaire mon chère Watson.

I.3. Le contrôle d'intégrité

Nous passerons rapidement ce point, puisqu'il s'agit d'une méthode liée à la détection d'activitées de post-exploitation d'une machine. Il faut juste savoir qu'elle existe.

Comme le titre l'indique, rien de très sexy. L'antivirus stock un fichier local comportant une liste des applications installés, avec leurs tailles, dates de modifications et les sommes de contrôles. Quand nous exécutons une application, la somme de contrôle théorique de celle-ci est calculée à partir des précédents scans, et si elle diffère de la réalitée, une petite alerte nous informera !
Ceci permet de vérifier si une application légitime est modifiée au cours du temps.

I.4. L'Analyse heuristique

Là où l'analyse par signature reconnaît uniquement les virus déjà croisés, l'analyse dynamique (ou heuristique) va théoriquement permettre de détecter les "nouveaux" virus. Quand un exécutable est analysé dynamiquement, l'AV va essayer de trouver des paternes d'altération de signature et surtout, observer le fonctionnement du code derrière l'exécutable.

Prenons un exemple concret. Un virus polymorphe est le parfait candidat pour outrepasser les techniques énumérées jusque là. En effet, le principe même de ce malware réside dans sa capacitées à modifier lui-même sa signatures !
De quoi laisser derrière lui des centaines de signatures uniques, qui ne correspondent à rien.
Pour détecter ce type de malwares, l'antivirus va faire quelque chose d'édifiant. Ce dernier va désassembler le malware, l'évaluer et observer si le programme essais de se lire et d'écraser du nouveau code au même endroit !
De cette façon, nous obtenons la signature dynamique d'une code polymorphe : nous abandonnons la comparaison pure des chaînes de caractères pour se concentrer sur des paternes de fonctionnement types.

Ce type d'analyse reste tout de même assez expérimentale, et ne retourne jamais de menaces avérés, mais uniquement des "fichiers suspects". Il est en effet difficile pour un antivirus d'étiqueter un fichier uniquement sur la base d'une analyse heuristique...
D'autant plus que ce type d'analyse à la particularité de générer un tas de faux positifs !

I.5. L’Analyse comportementale

Ici encore, tout est dans le titre !
Nos copains les antivirus regardent également ce que trifouillent les applications en arrière plan : ce qu’elles ont modifiées, à quoi elles cherchent à accéder, etc …
De cette façon, les AV traquent les applications, et observent si elles essaient de supprimer trops de choses, de modifier nos logs ou d’accéder à des dossiers “sensibles” par exemple.

C’est d'ailleurs sur cette fonctionnalitée que s'appuie les vagues de protections anti-ransomware proposés par certaines marques. L’antivirus comporte une règle relative à son analyse comportementale qui bloquera une application qui cherche à chiffrer trop de documents à la fois !

A noter pour plus tard que l’analyse heuristique et l’analyse comportementale sont faites dans la sandbox.

Nous avons maintenant fait le tour des principales fonctionnalitées des antivirus. Il faut bien les comprendres pour espérer les contourner par la suite. Retenez également que les différents antivirus sur le marché sont assez inégaux dans leurs fonctionnalités et dans le contenu de leurs bases de signatures statiques et dynamiques !